

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2006/300146

International filing date: 10 January 2006 (10.01.2006)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2005-003596
Filing date: 11 January 2005 (11.01.2005)

Date of receipt at the International Bureau: 07 April 2006 (07.04.2006)

Remark: Priority document submitted or transmitted to the International Bureau in
compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2005年 1月11日

出 願 番 号
Application Number: 特願2005-003596

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

J P 2005-003596

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

出 願 人
Applicant(s): 松下電器産業株式会社

2006年 3月23日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】 特許願
【整理番号】 7048060184
【提出日】 平成17年 1月11日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 11/14
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 田磨 雅基
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 佐藤 光弘
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 竹内 康雄
【発明者】
 【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 【氏名】 鶴切 恵美
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】特許請求の範囲

【請求項 1】

外部機器からの指示を受けてカード発行を行うセキュアデバイスであって、

前記セキュアデバイスは、

前記カード発行のためのコマンド群を保持するコマンド格納部と、

前記セキュアデバイスの動作を管理するカード管理部と、

前記外部機器からの指示を受けて、前記コマンド格納部が保持するコマンド群にもとづいて、前記指示を満たす一連の発行コマンドを選択、構築するカード発行部と、

を備え、

カード発行は、

前記カード発行部による前記発行コマンドの出力と、

前記発行コマンドを受けたカード管理部によるレスポンスと、

からなる、セキュアデバイス内部の通信のみによって実行され、

前記カード管理部は、発行処理結果を前記外部機器に対し出力することを特徴とするセキュアデバイス。

【請求項 2】

前記外部機器からの指示がカード発行要求かそれ以外かを判別し、カード発行要求の場合は、カード発行実行中は前記外部機器に発行処理結果を出力することができない特権モードを前記カード管理部に設定する特権モード管理部を更に備えることを特徴とする請求項 1 に記載のセキュアデバイス。

【請求項 3】

前記特権モード管理部は、前記カード発行が成功したことを確認した場合または、前記カード発行が途中で失敗した場合に、前記特権モードを解除することを特徴とする請求項 2 に記載のセキュアデバイス。

【請求項 4】

前記カード発行部は、カード発行の進捗状態を逐次、記憶し、カード発行の失敗を検出した場合は、失敗を意味する旨と発行処理の進捗状態とを、前記外部機器に出力することを特徴とする請求項 1 に記載のセキュアデバイス。

【請求項 5】

通信接続されたセキュアデバイスに対しカード発行を指示する外部端末であって、

発行処理の進捗状態を、前記セキュアデバイスから受け取るレスポンス受信部と、

前記発行処理の進捗状態に対応する該外部機器の動作を決定するセルフ発行管理部と、

前記セルフ発行管理部からの指示を受けて前記セキュアデバイスに対するコマンドを生成するコマンド生成部と、

前記コマンド生成部により生成されたコマンドを前記セキュアデバイスに送信するコマンド送信部と、

を備えたことを特徴とする外部機器。

【請求項 6】

前記コマンド格納部の発行コマンドを格納する領域を、直接アクセス可能な直接参照手段を更に設け、

前記指示がカード発行を意味する場合に、前記カード管理部が、前記直接参照手段を介して前記領域から発行コマンドを取得することを特徴とする請求項 1 に記載のセキュアデバイス。

【請求項 7】

前記カード管理部は、カード発行が中断したときの進捗状況を前記カード発行部に送る中断履歴送信手段を有し、

前記カード管理部は、前記中断履歴送信手段から受信した進捗状況をもとに最初に処理すべき発行コマンドを選択、構築するリカバリ手段を有することを特徴とする請求項 1 に記載のセキュアデバイス。

【書類名】明細書

【発明の名称】セキュアデバイス及び外部機器

【技術分野】

【0001】

本発明は、IC(Integrated Circuit)カードに代表されるセキュアデバイス並びに、セキュアデバイスに接続される携帯端末に代表される外部機器に関するものである。特に、通信接続された外部機器からの指示を受けて自立的にカード発行処理を行うセキュアデバイスに関するものである。

【背景技術】

【0002】

現在セキュリティデバイスとしてICカードが着目されている。ユーザの利便性の向上、ICカードによるサービスを提供したい事業者の参入障壁を下げることを目的に、カード発行後にアプリケーションをダウンロードすることが可能なマルチアプリケーション対応カードの開発が行われている。

【0003】

また、ICカードのようなセキュリティデバイスをモバイル機器に登載し、アプリケーションのダウンロードやアプリケーション利用を、モバイル機器を介して実施することが実用化されつつある。

【0004】

ここで、ICカードのハードウェア構成について概観する。

【0005】

図26は、ICカードのハードウェアに関する機能ブロック図である。ICカード2601は、CPU(Central Processing Unit)2602、ROM(Read Only Memory)2603、揮発性メモリ(例:RAM:Random Access Memory)2604、揮発性メモリ(例:EEPROM:Electrically Erasable Programmable Read Only Memory)2605、I/O IF2606を備えている。CPU2602は、演算を行う。ROM2603は書き換えができない読み出し専用のメモリである。ROM2603に格納される内容は、ICカード製造時に決定され、その後変更することはできない。RAM2604は読み書きが可能なメモリである。EEPROM2605は電源が切断されても内容が保持されるようになっている。I/O IF2606は、ICカードと外部とのデータ交換を担当する。CPU2602で実行されるプログラムは、通常「アプリケーション」と呼ばれる。アプリケーションの実行のためのコードは、ROM2603やEEPROM2605に格納される。また図26に示す以外に、ICカードが暗号操作のため暗号用コプロセッサを備える場合もある。

【0006】

ICカードに登載されるアプリケーションと外部(リーダ)は、ISO/IEC7816-4で規定されているAPDU(Application Protocol Data Unit)を使ってデータを交換する。APDUは、リーダがICカードに与えるコマンドと、ICカードからリーダに返すレスポンスの2つの構成からなる。

【0007】

図27はAPDUコマンド2701を示しており、ヘッダと本体から構成される。本体は、任意の長さで、空白の場合はなくともよい。ヘッダは、クラス(CLA)、命令(INS)とパラメータ1と2(P1, P2)で構成されている。

【0008】

APDUコマンドはCLA, INS, P1, P2, Lc 各1バイト、データ部: 255バイト、Le: 1バイトの合計261バイトが最大であり、アプリケーションをダウンロードするときの数Kバイトにおよぶデータを送信するためには、複数のAPDUブロックにわけて、それぞれのブロックのP1やP2でブロック番号やあとに続くブロックがあるかどうかを示すことにより、ICカード側で送られてきたコマンドの順番の整合性や最

終処理の必要性をチェックすることができる（図28参照）。

【0009】

LCを3バイトで表記し、1バイト目で3バイト表記であることを示し、2バイト目3バイト目でデータ長を示す拡張が提案されているが、ICカードのメモリ容量の観点から実装例はきわめて少ない。

【0010】

一般的にICカードのようなメモリ容量の小さなデバイスにおいては、受信したコマンドを格納する入力バッファは大きなサイズを取ることができない。マルチアプリケーション対応カードを用いて説明すると、ある領域を永続的に入力バッファとし、アプリケーション間で共通利用することで確保するメモリ容量を制限している。マルチアプリケーションカードでは、アプリケーションが選択されたときに「現在選択されているアプリケーションを示すカレントAP情報」を更新し、次につづくコマンドを受信したときにカレントAP情報を参照することにより、選択中のアプリケーションに確実にコマンドを渡すことができる。

【0011】

アプリケーションのダウンロードは、カードマネージャを介して行う。カードマネージャはマルチアプリケーション対応カードにおいてカードの管理やカード内のアプリケーションを管理するアプリケーションである。「カードの管理」とは、カード発行者がカードを管理するために必要なIDや鍵をカード内に格納するカード発行や、発行後のカードを一時停止状態や廃棄状態に移転させることである。また「アプリケーションの管理」とは、アプリケーションのダウンロードや削除をおこなうことである。

【0012】

また最近では、ICチップから大容量メモリをICカード拡張メモリ保護領域として利用可能なデバイス（以下、セキュアメモリカード）が提案され、ICカードアプリケーションデータの大容量化ニーズに対応可能となる。セキュアメモリカードは、モバイル機器の大きさに適合することから、スロット付きのモバイル機器に直接挿入し、モバイル機器を利用したEC（Electronic Commerce）サービス利用への展開が期待されている。

【0013】

モバイル機器を利用する場合には、電波圏外に位置することによって通信中断が起こり、その結果としてカードの振る舞いに影響を与える可能性が高くなる。通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理が提案されている。

【特許文献1】特開2003-108384号公報

【発明の開示】

【発明が解決しようとする課題】

【0014】

既存技術においてICカードやセキュアメモリカードなどのセキュアデバイスにアプリケーションをダウンロードする場合に、外部機器側でアプリケーションを複数のAPDU（Application Protocol Data Unit）ブロックに分割して送信する必要がある。セキュアデバイスのメモリ容量増加に伴って高機能アプリケーションが期待され、アプリケーション自体が巨大化する傾向にあり、その結果APDUブロック数はますます多くなる。

【0015】

モバイル機器を利用する場合には、電波圏外に位置することによって通信中断が起こり、その結果としてカードの振る舞いに影響を与える可能性が高くなる。APDUブロック数の増加はダウンロードが完了するまでに通信中断が発生する可能性が高くなることを意味する。通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理が提案されているが、再送中の失敗による再再送など繰り返し処理によるシステムやカード処理の複雑性、ダウンロード時間の増加によるユーザス

トレスが懸念され、できるだけ通信中断の影響を受けない方式が求められる。

【0016】

また、カード発行やアプリケーションダウンロードを行う際、種々のセキュリティ対策を行っている。具体的には通信経路上での盗聴を防止し、改竄を検知するためにAPDUブロックごとに暗号化やMAC (Message Authenticate Code) 付与を行い、カードに送信する。カードでは、APDUブロックの復号化やMAC検証を実施しているが、カードの処理能力を鑑みると 従来のセキュリティを確保しつつ、すべて平文処理もしくは復号化やMAC検証の回数を減らすことが可能な方式がのぞましい。

【0017】

さらに、カード発行やアプリケーションダウンロード時にカードとセッション鍵を共有し、そのセッション鍵でカードに送信するAPDUブロックの暗号化やMACを行うためには、元データとなるAPDUブロックを知る必要がある。

【0018】

APDUブロック作成者と、カード発行やアプリケーションダウンロードを実行する事業者が分離している場合があり、APDUブロックに個人情報を含む場合にはカード発行やアプリケーションダウンロードを実行する事業者がAPDUブロックの内容を知ることができない方式が期待されている。

【0019】

本発明は、こうした従来の問題点を解決するものであり、外部機器とカード間の通信回数を削減し、かつ従来のセキュリティを確保したうえでのカード内セキュリティ処理負荷を軽減することによって外部機器とカード間におけるデータ処理（例：カード発行やアプリケーションダウンロード）の高速化を目的としたものである。

【0020】

また本発明を利用することによって、カード発行やアプリケーションダウンロードに関与する複数の事業者間において契約によって実現されてきた情報保護を技術的に実現することができる。

【課題を解決するための手段】

【0021】

本発明のセキュアデバイスは、上記課題を解決するものであり、カード発行のためのコマンド群を保持するコマンド格納部と、前記セキュアデバイスの動作を管理するカード管理部と、外部機器からの指示を受けてコマンド格納部が保持するコマンド群にもとづいて、外部機器からの指示を満たす一連の発行コマンドを選択、構築するカード発行部とを備え、カード発行は、前記カード発行部による前記発行コマンドの出力と前記発行コマンドを受けたカード管理部によるレスポンスからなる、セキュアデバイス内部の通信のみによって実行されるセキュアデバイスである。

【0022】

コマンド格納部が予めカード発行のためのコマンド群を保持し、カード発行の際はカード内部の通信のみによってカード発行を実現することで、通信中断による発行処理の中断を防ぐとともに、外部機器から受信した信号を復号化するための処理負荷を軽減させることができる。

【0023】

また、本発明のセキュアデバイスは、外部機器からの指示がカード発行要求かそれ以外かを判別し、カード発行要求の場合は、前記外部機器に発行処理結果を出力することができない特権モードを前記カード管理部に設定する特権モード管理部を備えたものである。

【0024】

この特権モード管理部により、カード発行中の外部機器からの割り込みや外部機器への誤った出力を防ぐことができる。この場合、発行が終わった後にカードへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除され、以降外部機器からのコマンド送信が可能となる。

【0025】

また、本発明のセキュアデバイスは、カード発行が成功したことを確認した場合または、カード発行が途中で失敗した場合に、特権モードを解除する特権モード管理部を備えたものである。

【0026】

この特権モード管理部により、特権モードを解除するために外部機器からのアクションが必要なく、カード発行が終わった直後に外部機器からのコマンドを受信することができる。

【0027】

また、本発明のセキュアデバイスは、カード発行の進捗状態を逐次、記憶し、前記カード発行の失敗を検出した場合は、失敗を意味する旨と発行処理の進捗状態と、を外部機器に出力することを特徴とするカード管理部を備えたものである。

【0028】

このカード管理部により、セルフ発行が失敗した場合に外部機器がレスポンスを解析することによって発行がどこまで成功していたかを認識することができる。

【0029】

また、本発明の外部機器は、発行処理の進捗状態を前記セキュアデバイスから受け取るレスポンス受信部と、発行処理の進捗状態に対応する外部機器の動作を決定するセルフ発行管理部を備えたものである。

【0030】

カードビジネスでは、カード発行データを準備する事業者と、カード発行を担当する事業者が異なる場合が多い。このセルフ発行管理部により、エラーが発生した場合に実際にカードが処理したコマンドを外部に知られることなく、リカバリ処理が可能となる。

【0031】

また、本発明のセキュアデバイスは、前記コマンド格納部の発行コマンドを格納する領域を、直接アクセス可能な直接参照手段を更に設け、前記指示がカード発行を意味する場合に、前記カード管理部が、前記直接参照手段を介して前記領域から発行コマンドを取得することを特徴とするものである。

【0032】

この直接参照手段により、コマンドを分割して処理する場合と比較して、コマンド共通の定型処理や、次のコマンド処理用の準備プロセスを削減し、高速化が可能となる。

【0033】

また、本発明のセキュアデバイスは、前記カード管理部はカード発行が中断したときの進捗状況をカード発行部に送る中断履歴送信手段を有し、前記カード管理部は、前記中断履歴送信手段から受信した進捗状況をもとに最初に処理すべき発行コマンドを選択、構築するリカバリ手段を有することを特徴とするものである。

【0034】

中継履歴送信手段とリカバリ手段により、セキュアデバイスへの電源供給が起きたときの進捗状況を意識することなく再試行を実施することができるため、カード発行の負荷が減少する。

【発明の効果】

【0035】

以上、本発明により、外部機器とカード間の通信回数を削減し、かつ従来のセキュリティを確保したうえでのカード内セキュリティ処理負荷を軽減することによって外部機器とカード間におけるデータ処理（例：カード発行やアプリケーションダウンロード）の高速化を実現することができる。

【発明を実施するための最良の形態】

【0036】

以下、本発明の実施形態について図を用いて説明する。なお、本発明はこれら実施形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実

施しうる。

【0037】

以下の実施形態ではセキュアデバイスの例としてマルチアプリケーション対応カードを、発行の例としてアプリケーションダウンロードを採用して説明する。

【0038】

(実施の形態1)

本実施の形態を図1から図3を用いて説明する。

【0039】

図1は、本実施の形態におけるセキュアデバイス101の構成を示したブロック図である。カード管理部102は、外部機器105と通信を行い、セキュアデバイス101の動作を管理する。カード発行部103は、外部機器105からの指示を受けて、コマンド格納部104が保持するコマンド群にもとづいて、指示を満たす一連の発行コマンドを選択、構築する。コマンド格納部104は、カード発行のためのコマンド群を保持する。外部機器105は、セキュアデバイスにカード発行用の指示を送出する。

【0040】

セキュアデバイス101は、カード管理部102においてアプリケーションが選択されたときに「現在選択されているアプリケーションを示すカレントAP情報」を更新し、次につづくコマンドを受信したときにカレントAP情報を参照することにより、選択中のアプリケーションに確実にコマンドを渡すことができる。

【0041】

図2は、本実施の形態における外部機器105、カード管理部102、カード発行部103の処理フローを示したものである。

【0042】

外部機器105がカードマネージャを選択するためのコマンドを送信する。カード管理部102で選択に成功した場合、現在選択されているAPを示す「カレントAP情報」を「カードマネージャ」に更新し、次につづくコマンドを受信したときにカレントAP情報を参照することにより、カードマネージャに確実にコマンドを渡すことができる(STEP1:アプリケーション選択)。

【0043】

次に、コマンドを送信する外部機器105をセキュアデバイス101が認証する外部認証や、外部機器105がセキュアデバイス101を認証する内部認証を、必要とするセキュリティのレベルに応じて両方、あるいは一方のみ実施する(STEP2:認証)。

【0044】

次に、ダウンロードに必要なAPDUコマンドをまとめたデータ(以下、「連立コマンド」301と称する)をコマンド格納部104のセキュア領域に書き込む(以下、「ダイレクトアクセス」と称する)。ダイレクトアクセスでは一度に数メガバイトの書き込みが可能であるため、ダウンロードに必要な連立コマンドは通常一回だけのカードアクセスで書き込みが完了する(STEP3:ダイレクトアクセス)。

【0045】

連立コマンド301の構成を図3に示す。連立コマンド301は、いくつかのAPDUコマンド304、306、308、310から成り立っているかを示す「APDU数」302と、APDUコマンド304、306、308、310が何バイトで構成されているかを示す「コマンド長」303、305、307、309と、APDUコマンド304、306、308、310からなるデータが複数連なった「コマンド実体部」311から成る。それぞれの役割については後述する。

【0046】

次に外部機器が連立コマンド301を利用した発行を開始するための「セルフ発行開始コマンド」を送信する。

【0047】

図4は、セルフ発行開始コマンド401の形式の一例を示した図である。

【0048】

セルフ発行開始コマンド401は、セルフ発行開始コマンドであることを特定するためのヘッダ部402と、データ部403、404、405から構成される。

【0049】

セルフ発行開始コマンドのデータ部403、404、405は、コマンド格納部104内に存在する連立コマンド301を格納したファイルを特定するためのファイル特定情報（例えばファイル名やファイルIDなど）403と、特定したファイルからの読み出し位置を示すオフセット404、読み出すデータ長405から構成される。ただし、連立コマンドを格納するファイルが一意に決まっているなどの理由でデフォルト処理が可能な場合は、ファイル名やファイルIDなどを含む必要はない（STEP4：セルフ発行開始コマンド）。

【0050】

図5は、セルフ発行開始コマンド401を受信してから発行コマンドの読み出しを開始するまでのセキュアデバイス内部の動作フローである。

【0051】

カード管理部102はセルフ発行開始コマンド401を受信した後、ヘッダ部402を解析してセルフ発行開始コマンドであることを確認する（STEP501）。

【0052】

次に、カード管理部内に保持するファイル管理テーブル601（後述）を参照して、ファイルを特定するための情報403に対応するアドレスを特定する（STEP502）。

【0053】

図6はファイル管理テーブル601について示したものである、ファイル管理テーブル601は、ファイル名、ファイルのバス、ファイルを特定するための情報、ファイルサイズ、ダイレクトアクセス可能／不可能を示すダイレクトアクセス可能フラグ、アドレスが記述されており、それぞれの内容はファイルを作成したときに追加される。

【0054】

カード管理部102は、発行コマンドを受信した後にレスポンスを送信しない限り、次のコマンドを受信することができない。

【0055】

ここでは、セルフ発行開始コマンド401に対するレスポンスをカード発行部103に対して出力する。この場合、セルフ発行開始コマンド401に対するレスポンス（以下、セルフ発行トリガと称する）は、カード発行部103にとって連立コマンド301を処理するためのトリガとなる（STEP5：セルフ発行トリガ）。

【0056】

セルフ発行トリガには、アドレス、オフセット404、データ長405が含まれる。

【0057】

カード発行部103では、アドレスとオフセット404から物理的な読み出し位置を特定する（STEP503）。

【0058】

以後、連立コマンド301の読み出しを開始する（STEP504）。読み出し可能な連立コマンド301の長さは、セルフ発行開始コマンド401に含まれる読み出すデータ長405以下でなくてはならない。

【0059】

カード発行部103は、セルフ発行トリガを受け取ると、コマンド長303で指定された長さだけ連立コマンド301から最初のAPDUコマンド（例：INSTALL FOR LOAD）304を抽出し、カード発行部内のAPDUバッファにAPDUコマンドをコピーする。カード発行部では、APDUコマンドを抽出しAPDUバッファにコピーするたびに、カード発行部で管理する「既出コマンド数」をインクリメントする。既出コマンド数は、セルフ発行トリガを受け取ったときにゼロになっている必要がある。

【0060】

カード管理部102からのレスポンスの送り先はカード発行部103となり、INST ALL FOR LOADが正常終了した場合は、正常終了を意味するステータスワード（例：9000h）をカード発行部103に送る。カード発行部では、ステータスワードが正常終了を意味することを確認し、連立コマンドから次のAPDUコマンド306（例：LOAD1）を抽出し、APDUバッファにAPDUコマンドをコピーする。以下、既出コマンド数がAPDU数と一致するまでこれを繰り返す（STEP6～STEPm：発行コマンド）。

【0061】

既出コマンド数がAPDU数302と一致することは、最後の発行コマンド310であることを意味する。この場合、カードマネージャが最後のコマンドを正常処理したときのレスポンス送信先は外部機器となる。

【0062】

またセルフ発行の途中でメモリが枯渇した場合などの異常が発生した場合は、カード発行部103が異常を意味するステータスワード（例：6A84h）であることを確認し、異常終了を意味するステータスワードをカード管理部102に送信し、カード管理部102は異常終了結果をレスポンス（6A84h）として外部機器105に送信する。

【0063】

以上、本実施の形態では、アプリケーションダウンロードにおける外部機器105とセキュアデバイス101間の通信を、アプリケーションダウンロード時にアプリケーションの大きさに比例して数回～数十回発生していた従来技術と比較して、ダイレクトアクセス（STEP3）と、セルフ発行開始コマンド（STEP4）の2回へと減らすことができる。これは、モバイル網利用による通信中断のリスクを大幅に減らすことになる。

【0064】

さらに、一般的なアプリケーションダウンロードでは、認証時（STEP2）に外部機器105とセキュアデバイス101でセッション鍵を共有し、その後外部機器側でAPDUコマンドに対して暗号化や、改ざんや連続したコマンドであるかを検知するためのMAC（Message Authentication Code）を付与する。外部機器から送られたAPDUコマンドはカード内で復号やMAC検証を行っている。

【0065】

本実施の形態では、外部認証や内部認証によってお互いを認証（STEP2）したあと、ダイレクトアクセス（STEP3）によってカード管理部102（カードマネージャ）のみがアクセス可能な領域に連立コマンド301を格納し、セルフ発行によって外部にデータを出すことなく、すべて耐タンパー性を有するセキュアデバイス内部でダウンロード処理が完結する。したがって、発行時の盗聴や改ざんを考慮する必要がないために暗号化やMACの付与は必要ない。この結果、カードマネージャは平文を処理するだけでよく、ダウンロード処理が高速になる。

【0066】

また、送信可能なAPDUコマンドの全体長が固定であるために、平文の場合は、暗号化やMACの付与を行ったときに比べて一回のAPDUコマンドで送信可能なデータが大きい。したがって平文を適用可能な場合は、トータルのコマンド発行数も少なくなり、ダウンロード処理の高速化に有効である。

【0067】

本実施の形態では、カード交付後にアプリケーションをダウンロードする場合について説明したが、カード交付前に複数アプリケーションのダウンロード用データを格納しておき、ユーザが希望するアプリケーションをセルフ発行することもできる。

【0068】

（実施の形態2）

本実施の形態2について図7及び8を用いて説明する。

【0069】

図7は、本実施の形態におけるセキュアデバイス701の構成を示したブロック図であ

る。

【0070】

図7におけるカード管理部102、カード発行部103、コマンド格納部104、外部機器105は、それぞれ図1におけるカード管理部102、カード発行部103、コマンド格納部104、外部機器105と同様である。

【0071】

特権モード管理部702は、「特権モード」を管理し、カード管理部102とカード発行部103と連携する。「特権モード」とは、セキュアデバイス内部で連立コマンドを利用したコマンドの送受信を行う（以下、「セルフ発行」と称する。）ためのモードであり、このモードが指定されている間は、セキュアデバイス701の接触インタフェースや非接触インタフェースを介して外部機器105のやりとりはできない。

【0072】

図8は、本実施の形態における外部機器105、カード管理部102、カード発行部103、特権モード管理部702の処理フローを示したものである。

【0073】

図8において、STEP1からSTEPmは、実施の形態1で述べた図2と同様である。STEP5にてカード管理部102からセルフ発行トリガをカード発行部103が受け取った後に、カード発行部103は、特権モード管理部702に特権モードへの変更を依頼する（STEP5-a）。あるいは、セルフ発行トリガをカード発行部103におくるときに、カード管理部102が特権モード管理部702に特権モードへの変更を依頼してもよい。

【0074】

特権モードの間、カード管理部102の処理結果（レスポンス）の送り先はカード発行部103となり、前述の発行コマンド304（INSTALL FOR LOAD）が正常終了した場合は、正常終了を意味するステータスワード（例：9000h）をカード発行部103に送る。カード発行部103では、ステータスワードが正常終了を意味することを確認し、連立コマンド301から次のAPDUコマンド（例：LOAD1）を抽出し、APDUバッファにAPDUコマンドをコピーする。以下、既出コマンド数がAPDU数302と一致するまでこれを繰り返す。

【0075】

既出コマンド数がAPDU数302と一致することは、最後の発行コマンド310であることを意味する。この場合、カード管理部102（カードマネージャ）が最後のコマンドを正常処理したときのレスポンス送信先は外部機器105となる。

【0076】

またセルフ発行の途中でメモリが枯渇した場合などの異常が発生した場合は、カード発行部103が異常を意味するステータスワードであることを確認し、異常終了を意味するステータスワード（例：6a84hh）をカード管理部102に送信し、カード管理部102は異常終了結果をレスポンス（6A84h）として外部機器105に送信する。

【0077】

一旦特権モードに遷移すると、セキュアデバイスへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除される。

【0078】

本実施の形態2では、特権モード管理部702にて特権モードに設定されている間は、カード管理部102による外部機器105からのAPDUコマンド受信、外部機器105へのレスポンス送信を監視することにより、セルフ発行中の外部機器105からの割り込みや外部機器105への誤った出力を防ぐことができる。この場合、発行が終わった後にセキュアデバイスへの電源供給停止や、他のアプリケーションの選択や現在選択されているカードマネージャの再選択によって特権モードが解除され、以降外部機器105からのコマンド送信が可能となる。

【0079】

（実施の形態3）

本実施の形態3について図7、図9から図12を用いて説明する。

【0080】

本実施の形態3におけるセキュアデバイスの構成は、実施の形態2と同様であり、図7に示したものである。

【0081】

図9は、本実施の形態における外部機器105、カード管理部102、カード発行部103、特権モード管理部701の処理フローを示したものであり、図9においてSTEP5-b以外はすべて図8のSTEPと同様である。

【0082】

特権モード管理部701は、「特権モード」を管理し、カード管理部102とカード発行部103と連携する。「特権モード」とは、カード内部で連立コマンドを利用したコマンドの送受信を行う（以下、「セルフ発行」と称する。）ためのモードであり、このモードが指定されている間は、セキュアデバイス701の接触インタフェースや非接触インタフェースを介して外部機器105とのやりとりはできない。

【0083】

図9において、STEP1からSTEPmは実施の形態1と同様である。STEP5にてカード管理部102からセルフ発行トリガをカード発行部103が受け取った後に、カード発行部103は、特権モード管理部701に特権モードへの変更を依頼する（STEP5-a）。あるいは、セルフ発行トリガをカード発行部103におくるときに、カード管理部102が特権モード管理部701に特権モードへの変更を依頼してもよい。

【0084】

一旦特権モードに遷移すると、セルフ発行が最後まで正常に終了するか（STEPm）途中で失敗したことをカード発行部103が認識し、特権モード解除依頼を特権モード管理部701に要求するまで特権モードは解除されない（STEP5-b）。

【0085】

ここでカード発行部103の動作について図10、図11を用いて説明する。図10は、カード発行部103がカード管理部102からのレスポンスを参照する方式を示した図である。図11は、カード発行部103のレスポンス解析以後の処理フローを示した図である。

【0086】

まず、カード発行部103がカード管理部102からレスポンスを受け取った状態になる（STEP1101）。これは、カード管理部102で保持するレスポンスバッファに格納されるデータをカード発行部103で保持するレスポンスバッファにコピーする方式（図10（a））や、カード管理部102で保持するレスポンスバッファに格納されるデータをカード発行部103が参照する方式（図10（b））がある。

【0087】

この状態はレスポンスの解析が可能な状態であり、レスポンスに含まれるステータスワードを、カード発行部103が保持するレスポンス判定テーブル1201と比較することによって直前にカード発行部103が発行したコマンド処理が成功したか、失敗したかをカード発行部103が判断する（STEP1102）。

【0088】

図12は、レスポンス判定テーブル1201の一例を示した図である。カード発行部103は、カード管理部102から受け取ったステータスワードとレスポンス判定テーブル1201とを対比し、受け取ったステータスワードが9000hであれば、コマンド処理成功と判断し、9000h以外であれば、コマンド処理失敗と判断する。

【0089】

成功した場合、発行処理を継続する。失敗した場合、特権モード解除依頼を特権モード管理部701に要求し（STEP1103）、レスポンスを外部に送信する（STEP1

104)。

【0090】

本実施の形態3では、特権モード管理部702にて特権モードに設定されている間は、カード管理部102が外部機器105からAPDUコマンドを受け取ったり、外部機器105にレスポンスを返却したりすることを監視することにより、セルフ発行中の外部機器105からの割り込みや外部機器105への誤った出力を防ぐことができる。また実施の形態2のように特権モードを解除するために外部機器105からのアクションが必要なく、セルフ発行が終わった直後に外部機器105からのコマンドを受信することができる。

【0091】

(実施の形態4)

本実施の形態4について図13から図16を用いて説明する。

【0092】

図13は本実施の形態におけるセキュアデバイス1301の構成を示したブロック図である。カード管理部102、カード発行部103、コマンド格納部104、外部機器105はそれぞれ図1で示したものと同様である。

【0093】

レスポンス演算手段1302はカード発行部103内に存在し、カード発行の失敗を検出した場合に、失敗を意味する旨と、発行処理の進捗状態を意味するレスポンスデータを作成する手段である。図14はレスポンス演算手段への入力と出力の関係を示した図である。

【0094】

実施の形態1において、「カード発行部103は、セルフ発行トリガを受け取ると、コマンド長303で指定された長さだけ連立コマンド301から最初のAPDUコマンド(例:INSTALL FOR LOAD)304を抽出し、APDUバッファにAPDUコマンドをコピーする。カード発行部103では、APDUコマンドを抽出しAPDUバッファにコピーするたびに、カード発行部103で管理する既出コマンド数をインクリメントする。既出コマンド数は、セルフ発行トリガを受け取ったときにゼロになっている必要がある。」と述べた。

【0095】

また、「またセルフ発行の途中で異常が発生した場合は、カード発行部103が異常を意味するステータスワードであることを確認し、異常終了を意味するステータスワードをカード管理部102に送信し、カード管理部102は異常終了結果を外部機器105に送信する。」と述べた。この場合、外部機器105はカード管理部102から通知される異常終了結果を見てセルフ発行が成功したのか、失敗したのかを判別することができる。

【0096】

本実施の形態では、セルフ発行が失敗した場合に外部機器105が「どこまで成功していたのか」を認識可能な方式について説明する。

【0097】

図15は、カード管理部102からレスポンスを受け取ったカード発行部103のレスポンス解析以後の処理フローを示した図である。ここでSTEP1101、1102、1104は実施の形態3で述べたフローと同様である。

【0098】

カード発行部103が異常を意味するステータスワードを、レスポンス判定テーブル1201により確認した後(STEP1101、1102)、カード発行部703はカード発行部103内部で保持しているレスポンス演算手段1302において、図14に示すように「既出コマンド数」と異常を意味するステータスワードを入力値として、レスポンスを生成し(STEP1503)、外部機器105に出力する(STEP1104)。

【0099】

レスポンスのフォーマットとしては、2バイトからなるステータスワードのいずれかのビットを利用する場合(例:63CXh(Xが既出コマンド数))や、図16に示すよう

に既出コマンド数（発行処理の進捗状態を示す）をデータ部1602に設定し、データ部1602とステータスワード（発行処理の失敗した旨を示す）1603からなるレスポンス1601としてもよい。

【0100】

本実施の形態では、カード発行部103にレスポンス演算手段1302を設けることにより、セルフ発行が失敗した場合に外部機器105がレスポンス1602を解析することによって発行がどこまで成功していたかを認識することができる。

【0101】

（実施の形態5）

本実施の形態5について図16から図19を用いて説明する。

【0102】

図17は本実施の形態における外部機器1701の構成を示したブロック図である。外部機器1701は、セルフ発行を制御し、正常か失敗かを判定した後に、該外部機器1701の次の動作を決定するセルフ発行管理部1702、コマンドを作成するコマンド生成部1703、コマンドを送信するコマンド送信部1704、レスポンスを受信するレスポンス受信部1705から構成される。従来のカード発行では、あらかじめ外部機器が作成した発行コマンドをカードに送信するため、カードから進捗状況を表すレスポンスを受け取る必要はない。外部機器がコマンドを送信し、異常を意味するレスポンスがカードから送られてきたら、異常が発生した原因となるのは直前に送信したコマンドである。

【0103】

本実施の形態では、外部機器1701は発行要求をセキュアデバイスに送信するのみであるため、セキュアデバイスから発行処理の進捗状態が返却されない限り、どこまでが正常だったかを知ることはできない。

【0104】

本実施の形態5では、セルフ発行開始コマンドをセキュアデバイスに送信し、実施の形態4で述べた失敗を意味する旨と発行処理の進捗状態を表すレスポンスをセキュアデバイスから受信した後の外部機器1701の挙動について説明する。

【0105】

セルフ発行を行う場合、セルフ発行管理部1702がコマンド生成部1703にセルフ発行開始コマンドの発行を要求する。コマンド作成部1703は、コマンド送信部1704を介してセキュアデバイスにセルフ発行開始コマンドを送信する。

【0106】

図18は、セキュアデバイスからレスポンスを受信した後の外部機器1701の処理フローを示した図である。なお、レスポンスデータのフォーマットは、実施の形態4で述べた図16を例として説明する。

【0107】

セキュアデバイスからのレスポンスをレスポンス受信部1705が受信すると（STEP1801）、セルフ発行管理部1702がステータスワードを参照し、例えば9000hであれば成功、それ以外なら失敗と判定する（STEP1802）。

【0108】

成功の場合、セルフ発行処理を終了する。また、セルフ発行は成功したが確認用のコマンドを外部機器1701から受け取った後に使用可能となる場合は、コマンド生成部1703に「カード使用許可確認用コマンド」を発行するように要求する。

【0109】

あるいは、外部機器1701にインターネット接続やモバイル通信用のインタフェースを設け、成功した結果を、別の外部機器に通知することもある。

【0110】

ステータスワードが失敗の場合、セルフ発行管理部1702は、レスポンスに含まれる既出コマンド数をキーにして、セルフ発行管理部1702が保持する進捗管理テーブル1901を参照する（STEP1803）。

【0111】

図19は、進捗管理テーブル1901の一例を示した図であり、セキュアデバイスから受け取ったレスポンスに含まれる「既出コマンド数」と、その「既出コマンド数」に対応する外部機器1701の処理内容が、「既出コマンド数」毎に記載されている。

【0112】

セルフ発行管理部1702は、セキュアデバイスから受け取ったレスポンスに含まれる「既出コマンド数」を抽出し、進捗管理テーブル1901を参照して、次の動作を決定する。

【0113】

レスポンス1601の既出コマンド数がnの場合には、進捗管理テーブル1901に従ってコマンド生成部1703に、発行中に書き込んだデータをすべてクリアするための「クリアコマンド」を要求する(STEP1804)。

【0114】

コマンド生成部1703は、従来のカード発行において外部機器がカードに送信する鍵やIDを設定するコマンドや、アプリケーション用のデータを設定するコマンドではなく、セルフ発行開始コマンドと、クリアコマンドやカード使用許可確認コマンドのような、セキュリティ保護が必要ない発行後処理コマンドを作成する。

【0115】

カードビジネスでは、カード発行データを準備する事業者と、カード発行を担当する事業者が異なることがある。

【0116】

提案する方式に適用すると、カード発行データを準備する事業者は図2、図8、図9においてSTEP3まで、カード発行を担当する事業者はステップ4以降を実施することになる。

【0117】

一般的に外部機器1701を用いてカード発行を担当する事業者は、どのようなカード発行データを用いてカード発行を実施しているかを知らないほうがセキュリティの観点で望ましい。

【0118】

本実施の形態では、どのようなコマンドを発行したかをカード発行担当事業者が知ることなく発行が完了するために、セキュリティ保護を実現できる。

【0119】

(実施の形態6)

本実施の形態を図20、図21、図3を用いて説明する。

【0120】

図20は、本実施の形態におけるセキュアデバイス2001の構成を示したブロック図である。

【0121】

図20におけるカード管理部102、カード発行部103、コマンド格納部104、外部機器105は、それぞれ図1におけるカード管理部102、カード発行部103、コマンド格納部104、外部機器105と同様である。2002はカード管理部に含まれ、コマンド格納するAPDUバッファ、2003は連立コマンドが格納された領域を、直接アクセス可能な直接参照手段である。2004は、コマンド格納部104の連立コマンドが格納された領域の一部を、連立コマンドのAPDUバッファとして、一時的に利用される連立コマンドAPDUバッファである。直接参照手段2003は、この連立コマンドAPDUバッファ2004を、直接参照することができる。

【0122】

図21は、本実施の形態における連立コマンドを示す。

【0123】

連立コマンド2101は、いくつかのAPDUコマンド2104、2106から成り立っ

ているかを示すAPDU数2102と、APDUコマンド2104、2106が何バイトで構成されているかを示す、コマンド長2103、2105と、APDUコマンド2104、2106からなるデータが複数連なった、コマンド実体部2111から成る。それぞれの役割については後述する。

【0124】

本実施の形態1から4では、セルフ発行開始コマンドにてカード発行部が連立コマンドを格納するファイルを特定し、ファイルに含まれるAPDUコマンドを抽出して、一旦、カード管理部102内のAPDUバッファにコピーすることによってカード管理部（カードマネージャはカード管理部の一部となる）は、APDUコマンドが外部機器から接触インタフェースや非接触インタフェースを介して送られてきたものか、セルフ発行によるものか、を区別することなくAPDUコマンドを実行する方法を述べた。

【0125】

本実施の形態6では、接触インタフェースや非接触インタフェースを利用する際のAPDUバッファ2002と、セルフ発行時のAPDUを格納するバッファとを共有しない形態について説明する。

【0126】

実施の形態1と同様にセルフ発行開始コマンドに対するレスポンス（以下、セルフ発行トリガと称する。）は、カード発行部103にとって連立コマンド2101を処理するためのトリガとなる。

【0127】

カード発行部103はセルフ発行トリガを受け取るとコマンド長2103で指定された長さだけ連立コマンド2101から最初のAPDUコマンド（例：INSTALL FOR LOAD）2104を抽出し、コマンド格納部104内にAPDUコマンド長さ分の領域をAPDUバッファとして指定する。

【0128】

このとき、外部機器105からのAPDUコマンドを格納するAPDUバッファ2002と連立コマンド用のAPDUバッファ2004が並存する。すなわち外部機器105からのAPDUコマンドを格納するAPDUバッファ2002はカード管理部に属し、連立コマンド用のAPDUバッファ2004はコマンド格納部104に属する。

【0129】

例えば最初のAPDUコマンド（INSTALL FOR LOAD）を処理する場合には、APDUコマンド2104で表す発行コマンド1-aが占める領域自体が連立コマンド用APDUバッファとなる。

【0130】

外部機器105からのAPDUコマンドを格納するAPDUバッファ2002が固定領域として永続するのに対して、連立コマンド用のAPDUバッファ2004は、あるコマンドを処理する瞬間のみ、そのコマンドが入っている領域を占めるものであり、次のコマンドを処理することによって時々刻々と領域のアドレスや大きさが変化する。すなわち、発行コマンド1が処理されたら次は、発行コマンド2-aが占める領域自体が連立コマンド用APDUバッファとなる。

【0131】

ここで実施の形態1における連立コマンドを示す図3と本実施の形態における連立コマンドを示す図21を比較する。図3においてLOADコマンドは発行コマンド2から発行コマンドmに分割されている。例えばダウンロード対象のデータが2000キロバイトであった場合、一回で送信可能な、つまりAPDUバッファ2002に格納可能なデータ長の最大が255バイトとすると（ただし平文の場合。暗号化やMAC付与の場合はより短くなる。）、 $255 \times 7 < 2000 < 255 \times 8$ となり8コマンドに分割して送る必要があるため、 $m=9$ となる。

【0132】

これに対し、図21においては、LOADコマンドを連立コマンド用APDUバッファ

2004で指定することで、一回の処理で完結させることができる。

【0133】

カードマネージャは、カード管理部102のAPDUバッファ2002からデータを取得する場合と同様に、直接参照手段2003を介することで連立コマンド用APDUバッファ2004からデータを取得する。いずれの場合もカードマネージャの挙動としては、APDUバッファにアクセスする点で等価な処理となる。

【0134】

直接参照手段2003を利用するタイミングは、セルフ発行開始コマンドを受信した後にカード管理部102から直接参照手段2003に要求する場合や、カード発行部103がセルフ発行トリガを受け取って、直接参照手段2003に要求してもよい。

【0135】

なお、特権モード管理部702を設けて、特権モードのときだけこの直接参照手段2003を利用可能としてもよい。

【0136】

次に、実施の形態1の場合のように複数回にわけてLOADコマンドを受信する場合と、本実施の形態の場合のように一回でLOADコマンドを受信する場合のカードマネージャの動作を説明する。

【0137】

複数回にわけてLOADコマンドを処理する場合、コマンド数分、APDUコマンド受信処理、APDUバッファからのデータ取得処理、そのコマンドが正しい順番で送られてきているか、最後のコマンドであるかのコマンドチェック、データの処理、次のコマンドを処理するための中間状態の保持、レスポンス送信処理が必要となる。

【0138】

一方、LOADコマンドを一回で処理する場合、APDUコマンド受信処理、APDUバッファからのデータ取得処理、コマンドチェック、レスポンス送信処理が一回だけとなり、また次のコマンドを処理するための中間状態の保持はいらない。

【0139】

このように、本実施の形態では直接参照手段2003を備えることで、コマンドを分割して処理する場合と比較して、コマンドごとに行う必要のある定型処理を大幅に減らし、また次のコマンドに備えるための冗長な処理をなくすことができる。この結果として、外部機器からAPDUを複数回にわけてダウンロードする従来のやり方に対して、大幅な高速化が可能となる。

【0140】

読み／書き機能を有する携帯電話等の可搬性の高いモバイル端末を用いてセキュアデバイスにアプリケーションをダウンロードする場合、一般的に電源となる電池容量が有限であることから高速化の意義は大きい。

【0141】

さらには、セキュアデバイスが携帯電話に抜き差しできるリムーバブルメディアの場合、ユーザが突然電源を切るケースやダウンロード処理途中にセキュアデバイスを抜くことによるセキュアデバイスへの電源供給停止が起こりうる。これらのケースにおいても、高速処理できることはユーザの誤った操作の影響をうける可能性が小さくなることを意味するため意義は大きい。

【0142】

(実施の形態7)

本実施の形態を図22から図24を用いて説明する。

【0143】

図22は、本実施の形態におけるセキュアデバイス2201の構成を示したブロック図である。

【0144】

図22におけるカード管理部102、カード発行部103、コマンド格納部104、外

部機器 105 は、それぞれ図 1 におけるカード管理部 102、カード発行部 103、コマンド格納部 104、外部機器 105 と同様である。2202 は実施の形態 1 から 6 で説明した既出コマンド数を保持し、カード発行部 103 に送信する中断履歴送信手段、2203 は中断履歴送信手段から受信した既出コマンド数に応じたリカバリを実施するリカバリ手段である。

【0145】

図 23 は本実施の形態における連立コマンドを示す。

【0146】

図 23 における 302 ～ 311 は、図 3 における 302 ～ 311 と同様である。

【0147】

連立コマンド 2301 は、図 3 で示した、いくつかの APDU コマンド 304、306、308、310 から成り立っているかを示す「APDU 数」302 と、リカバリを実施する際に参照するリカバリ情報 2302 と、APDU コマンド 304、306、308、310 がそれぞれ何バイトで構成されているかを示す「コマンド長」303、305、307、309 と、発行コマンド 304、306、308、310 からなるデータが複数連なった「コマンド実体部」311 とから成る。

【0148】

図 25 は、リカバリ情報 2302 の一例を示した図である。リカバリ情報 2302 は、リカバリ情報の長さを表すリカバリ情報長 2401 と、リカバリ時にどのコマンドから発行するかを示すコマンド番号 2402、2404 と、コマンド番号で特定される発行コマンドが連立コマンド 1302 のどの位置から始まっているかを表すオフセット 2403、2405 から構成される。なお、コマンド番号 2402、2404 とオフセット 2403、2405 は組となって複数設定することができる。

【0149】

カード発行途中にカードへの電源供給がなくなる（以下、電源断）とカードは処理を中止し、レスポンスを外部機器 105 に送信することはない。実施の形態 1 ～ 6 で述べてきたセルフ発行においてレスポンスが外部機器 105 に到達しないことは、電源断が生じたとき即座にカード発行の進捗状況を外部機器が知ることができないことを意味する。

【0150】

なお、電源断の検知については、例えば、セッションタイムアウトを利用することによって可能である。

【0151】

本実施の形態では、電源断を検知後、セキュアデバイス 2201 のリカバリ処理を実施について説明する。

【0152】

リカバリ処理は以下の 3 パターンに区分されるカード実装に依存する。

【0153】

7-1) 電源断発生後に、電源供給が発生したときや、最初のコマンドを受け取ったときに、電源断が生じるまでにセキュアデバイス 2201 内で確保した領域や格納したデータをすべてクリアする場合

この場合のリカバリ処理は、カード発行を最初からやり直すことになる。このような実装を施したセキュアデバイス 2201 は、カード管理部 102 が管理する既出コマンド数は RAM (Random Access Memory) などの一次記憶領域に保持しておけばよい。

【0154】

外部機器 105 も電源断を検知した後に発行が要求されたときにセルフ発行開始コマンドを送信すればよい。

【0155】

7-2) それまでに確保した領域や格納したデータはそのまま、電源断がおきたコマンドからやり直しができる場合（コマンド単位でリカバリ処理可能な場合）

この場合のリカバリ処理は、電源断がおきたコマンドからやり直すことになる。このような実装を施したセキュアデバイス 2201 では、電源断が発生した前回の処理において何番目のコマンドで失敗したかを記憶しておく必要がある。

【0156】

したがってカード管理部 102 が管理する既出コマンド数は、EEPROM などの不揮発性記憶領域に保持する必要がある。

【0157】

図 25 は、セキュアデバイス 2201 におけるリカバリ処理の動作を示したフロー図である。

【0158】

電源断発生後に外部機器 105 からセルフ発行コマンドが送信された場合、カード管理部 102 はセルフ発行コマンドであることを確認した後 (STEP 2501)、既出コマンド数がゼロでないことを確認する (STEP 2502)。ここで既出コマンド数がゼロでないことは、前回の発行が電源断によって中断されたことを意味する。

【0159】

次に、カード管理部 102 は既出コマンド数を中断履歴送信手段 2202 を介してカード発行部 103 に渡す (STEP 2503)。カード発行部 103 では、リカバリ手段 2203 が連立コマンド 2301 の一部であるリカバリ情報 2302 を検索し、既出コマンド数と一致するコマンド番号 2402、2404 を検索し、該当するコマンド番号が存在した場合にコマンド番号と対になる先頭からのオフセット 2403、2405 を抽出することで今回最初に送るべきコマンドを特定する (STEP 2504)。次に、特定したコマンドを読み出し、カード管理部の APDU バッファにコピーし発行が再開される (STEP 2505)。

【0160】

本方式ではリカバリ情報 2302 を参照することで読み出し位置を決定する内容について述べたが、リカバリ情報 2302 を付与せず図 3 で述べた連立コマンド 301 を先頭から解析することで読み出し位置を特定してもよい。たとえば、既出コマンド数が 2 であれば、コマンド長 303 が存在するアドレスを特定し、指定された長さをアドレスに加えて、コマンド長 305 が存在するアドレスを特定し、その後続く発行コマンド 2 (Load1) 306 の読み出し位置が決定されることになる。

【0161】

7-3) それまでに確保した領域や格納したデータはそのまま、あるいは「あるコマンド」処理以前に確保した領域や格納したデータがそのまま、「あるコマンド」以降からやり直しができる場合 (機能単位でリカバリ処理)

図 24 において、コマンド番号 1 (2402) に「1」、コマンド番号 2 (2404) に「2」が設定されているとする。

【0162】

発行コマンド 3 (Load2) 308 は 3 番目のコマンドであり、ここで電源断が発生した場合、カード管理部 102 が管理する既出コマンド数は「3」のまま EEPROM などの不揮発性記憶領域に保持されている。

【0163】

図 25 は、セキュアデバイス 2201 におけるリカバリ処理の動作を示したフロー図である。

【0164】

外部機器 105 からセルフ発行開始コマンドが送信された場合、カード管理部 102 はセルフ発行コマンドであることを確認した後 (STEP 2501)、既出コマンド数がゼロでないことを確認する (STEP 2502)。ここで既出コマンド数がゼロでないことは、前回の発行が電源断によって中断されたことを意味する。

【0165】

次に、カード管理部 102 は既出コマンド数「3」を中断履歴送信手段 2202 を介し

てカード発行部103に渡す(STEP2503)。

【0166】

カード発行部103のリカバリ手段2203では、既出コマンド数「3」とコマンド番号1(1402)に設定されている「1」、コマンド番号2(1404)に設定されている「2」と比較して、 $1 < 2 < 3$ の関係になることから、「3」より小さく、「3」に最も近い「2」からやり直すことを決定する(STEP2504)。

【0167】

次に、カード発行部103はコマンド番号2に該当する発行コマンド2(Load1)306を抽出してAPDUバッファにコピーし発行が再開される(STEP2505)。

【0168】

本実施の形態では、カード管理部102に中断履歴送信手段2202、カード発行部103にリカバリ手段2203を備えることで、カード発行途中にカードへの電源供給がなくなった場合の事後処理において再試行が可能となる。

【0169】

外部機器105は、カードへの電源供給が起きたときの進捗状況を意識することなく再試行を実施することができるため、カード発行の負荷が減少する。

【産業上の利用可能性】

【0170】

本発明のセキュアデバイスと外部機器は、外部機器からセキュアデバイスへ1度の指示を出すことにより、後はセキュアデバイス内で自立的に処理を実行することができるので、カードとの間の通信状態が不良の下でのカード発行や、ユーザが持っている携帯端末機器を利用して個人が自由にカード発行することに適している。

【図面の簡単な説明】

【0171】

【図1】 本発明の実施の形態1におけるセキュアデバイスのブロック図

【図2】 本実施の形態1における処理フロー図

【図3】 連立コマンドの一例を示す図

【図4】 セルフ発行開始コマンドフォーマットの一例を示す図

【図5】 セルフ発行コマンドを受信してから発行コマンドの読み出しを開始するまでのセキュアデバイス内部の動作フロー図

【図6】 ファイル管理テーブルの一例を示す図

【図7】 本発明の実施の形態2、3におけるセキュアデバイスのブロック図

【図8】 本実施の形態2における処理フロー図

【図9】 本実施の形態3における処理フロー図

【図10】 カード発行部がカード管理部からのレスポンスを参照する方式例を示す図

【図11】 レスポンス解析以後の処理フロー図

【図12】 レスポンス解析用の参照テーブルの一例を示す図

【図13】 本発明の実施の形態4におけるセキュアデバイスのブロック図

【図14】 レスポンス演算手段への入力と出力の関係図

【図15】 レスポンス解析以後の処理フロー図

【図16】 レスポンスデータフォーマットの一例を示す図

【図17】 本実施の形態5における外部機器の構成を示したブロック図

【図18】 レスポンスを受信した以後の外部機器における処理フロー図

【図19】 セルフ発行管理部が次の動作を決定するための進捗管理テーブルの一例を示す図

【図20】 本実施の形態6におけるセキュアデバイスの構成を示したブロック図

【図21】 本実施の形態6における連立コマンドの一例を示す図

【図22】 レスポンスデータフォーマットの一例を示す図

【図23】 本実施の形態7における連立コマンドの一例を示す図

【図24】 リカバリ情報の一例を示す図

【図25】リカバリを実施するときの処理フロー図

【図26】ICカードのハードウェアに関する機能ブロック図

【図27】APDUコマンドのフォーマット図

【図28】データを分割してAPDUを作成する方式の概念図

【符号の説明】

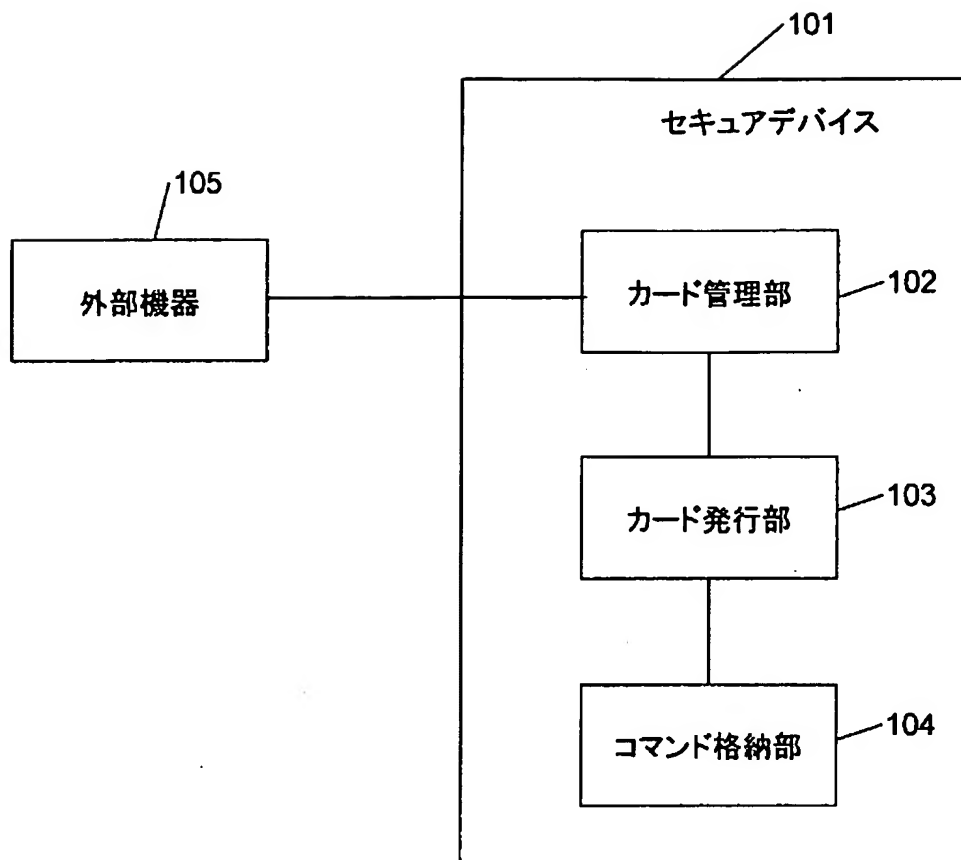
【0172】

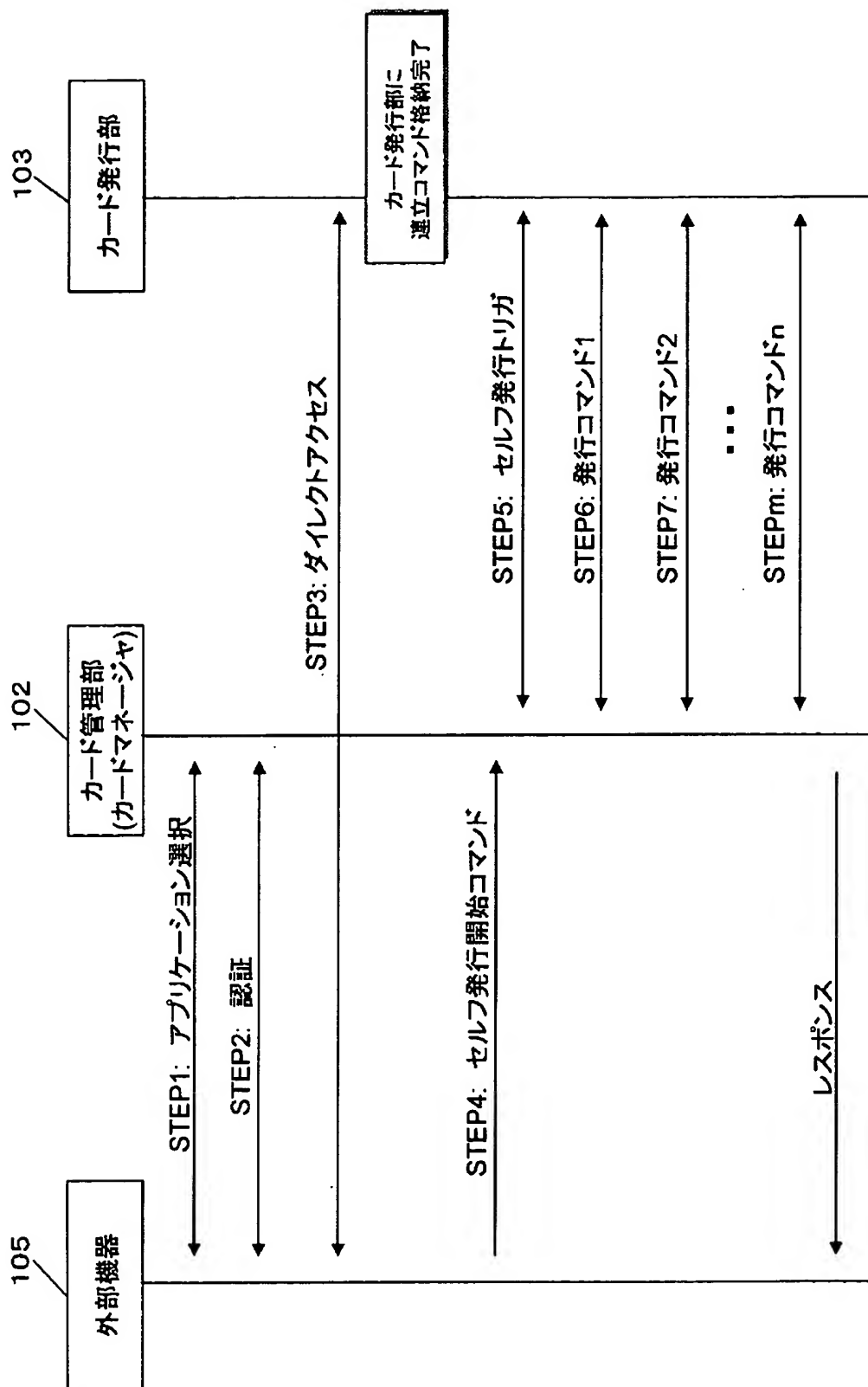
101	セキュアデバイス
102	カード管理部
103	カード発行部
104	コマンド格納部
105	外部機器
301	連立コマンド
302	APDU数
303, 305, 307, 309	コマンド長
304, 306, 308, 310	発行コマンド
311	コマンド実体部
401	セルフ発行コマンド
402	ヘッダ部
403	ファイル特定情報
404	ファイルからの読み出し位置(オフセット)
405	読み出すデータ長
601	ファイル管理テーブル
701	セキュアデバイス
702	特権モード管理部
1201	レスポンス解析用参照テーブル
1301	セキュアデバイス
1302	レスポンス演算手段
1601	レスポンス
1602	データ部
1603	ステータスワード
1701	外部機器
1702	セルフ発行管理部
1703	コマンド生成部
1704	コマンド送信部
1705	レスポンス受信部
1901	進捗管理テーブル
2001	セキュアデバイス
2002	APDUバッファ
2003	直接参照手段
2004	連立コマンド用APDUバッファ
2101	連立コマンド
2102	APDU数
2103, 2105	コマンド長
2104, 2106	発行コマンド
2111	コマンド実体部
2201	セキュアデバイス
2202	中断履歴送信手段
2203	リカバリ手段
2301	連立コマンド
2302	リカバリ情報

2401	リカバリ情報長
2402, 2404	コマンド番号
2403, 2405	オフセット
2601	ICカード
2602	CPU
2603	ROM
2604	RAM
2605	EEPROM
2606	I/O IF
2701	APDUコマンド

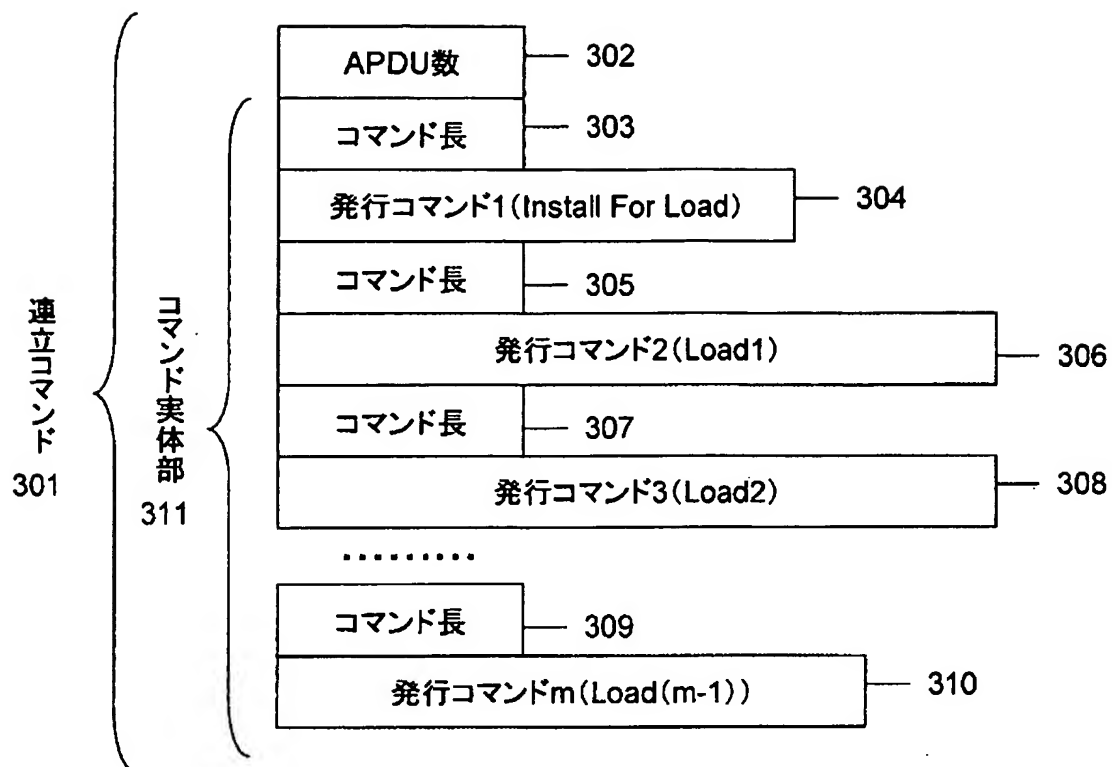
【書類名】 図面

【図 1】

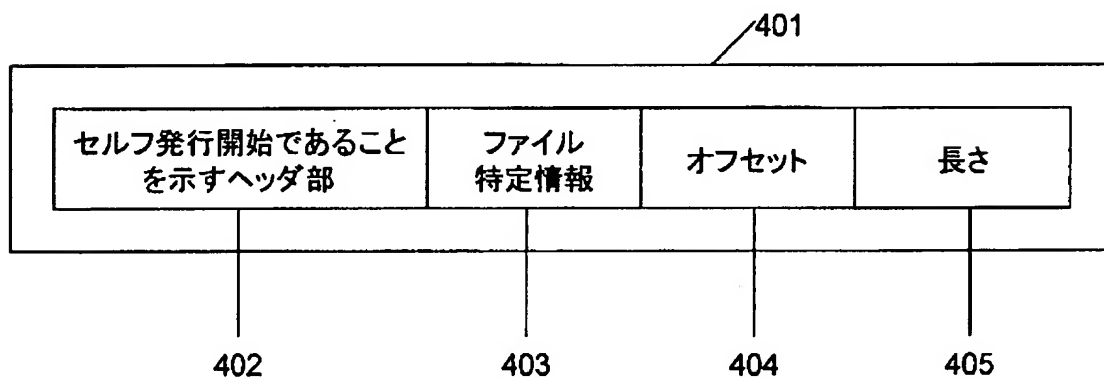




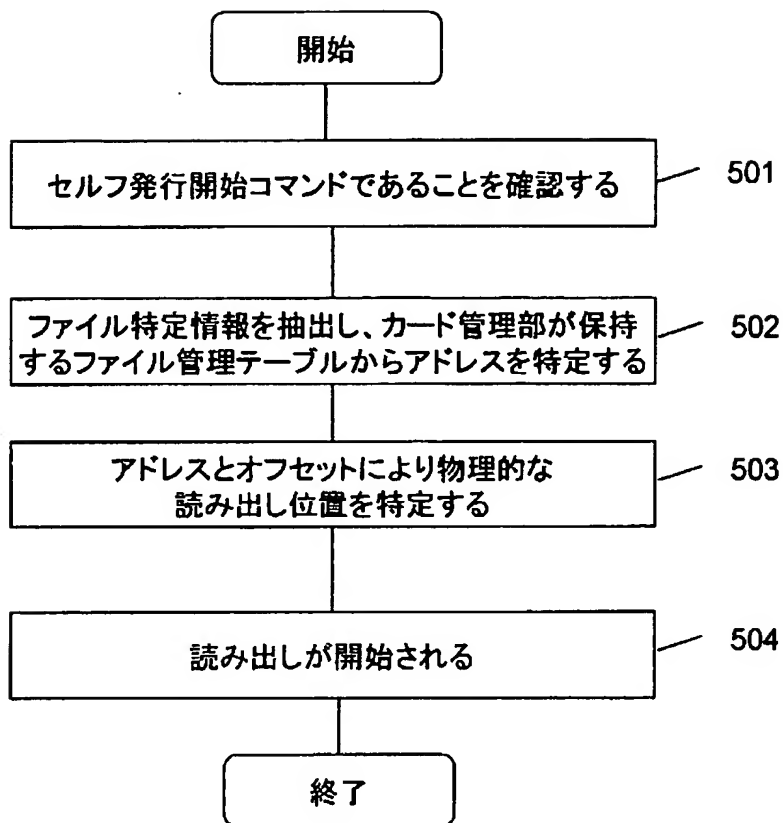
【図 3】



【図 4】



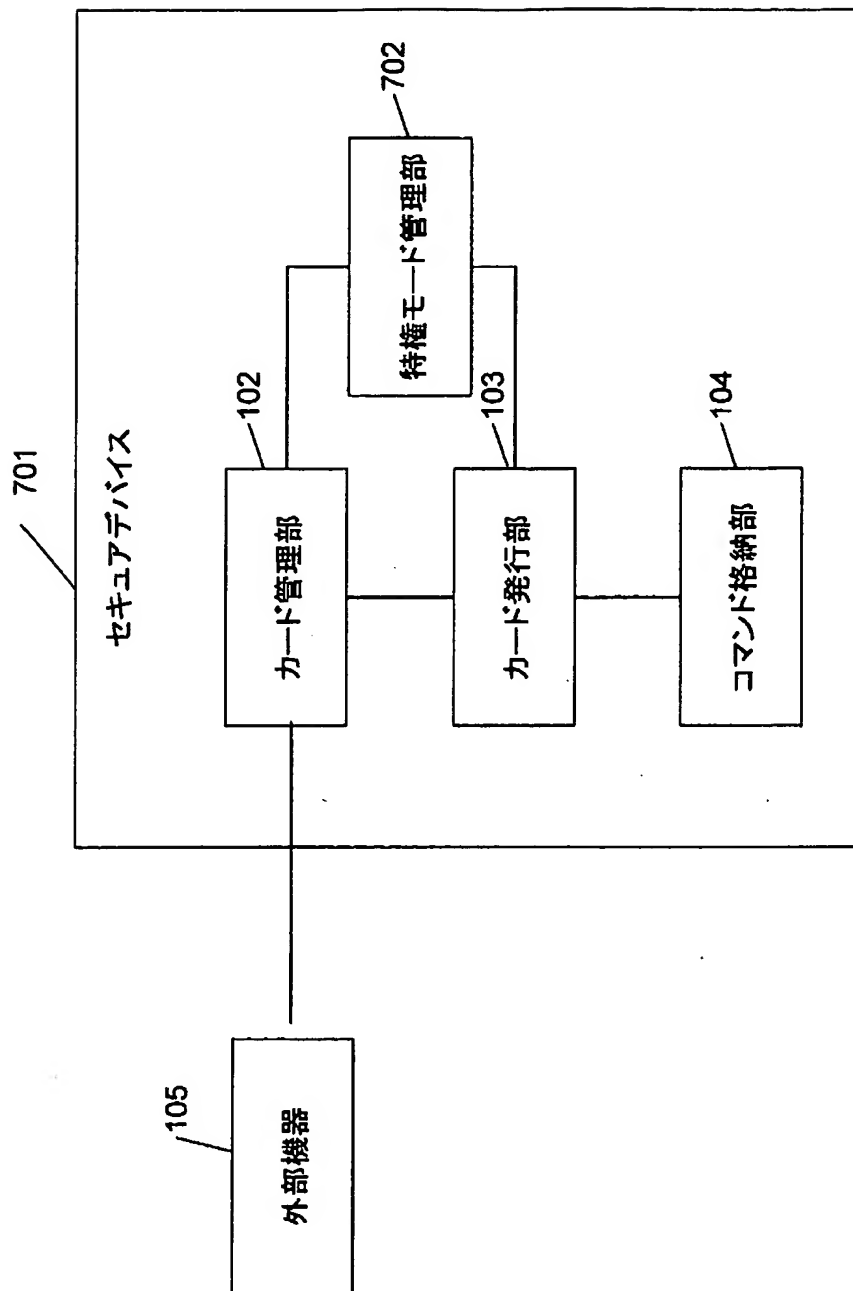
【図 5】

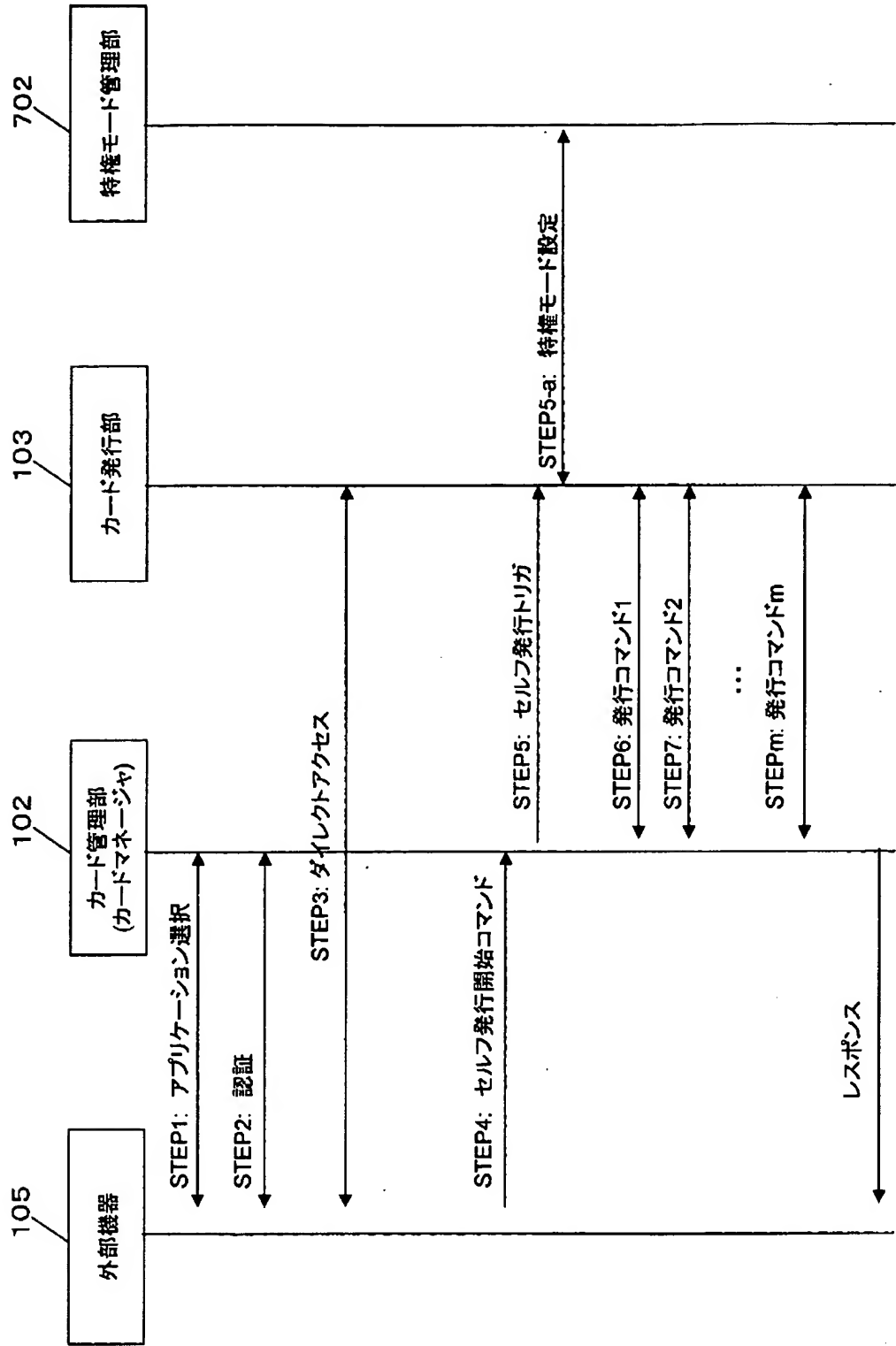


601

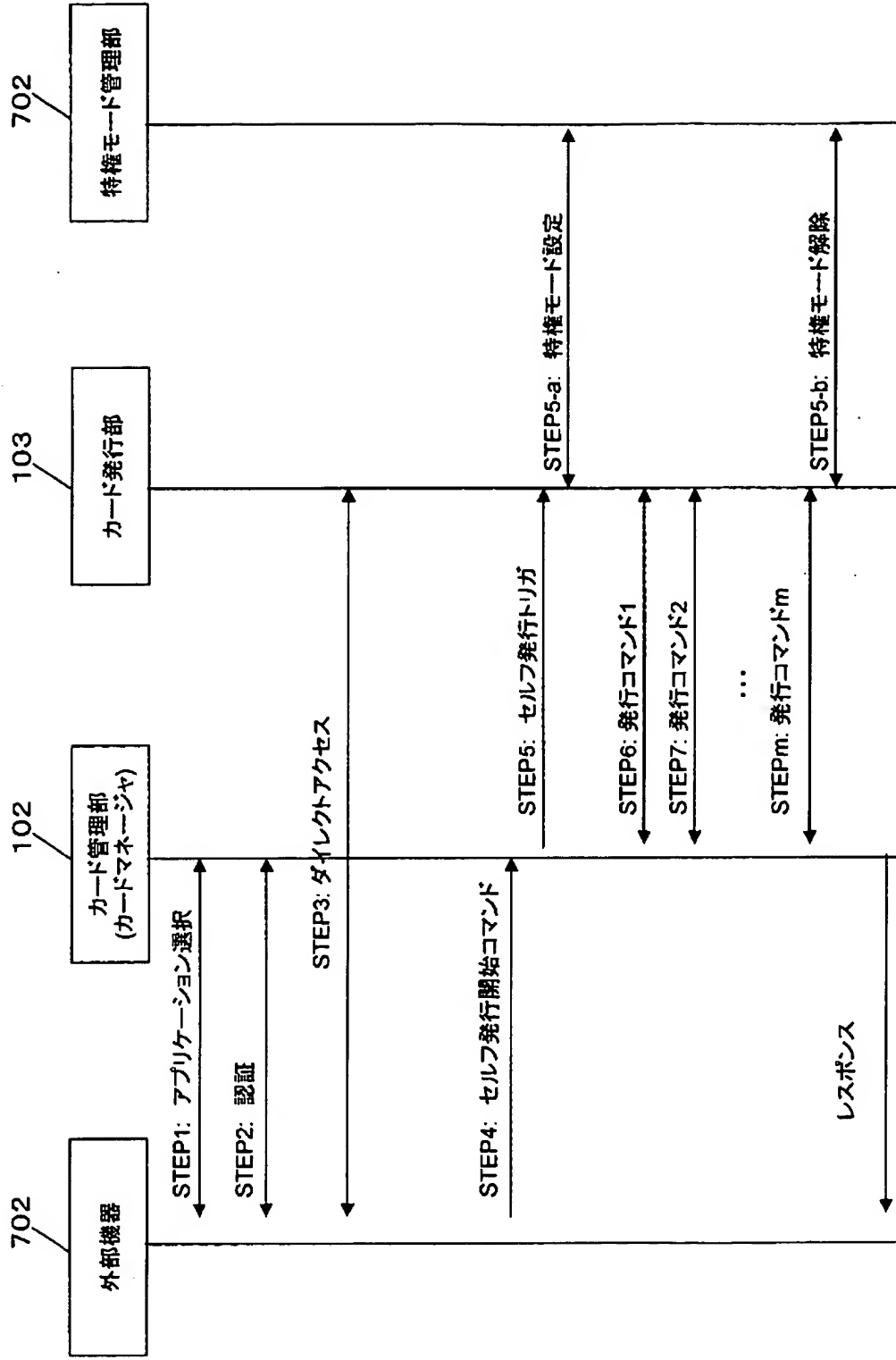
ファイル名	ファイルパス	ファイル特定情報	ファイルサイズ	ダイレクトアクセス可能フラグ	アドレス
File_1	Root/	1	a	true	****
File_2	Root/dir1	2	b	true	△△△△

【図 7】

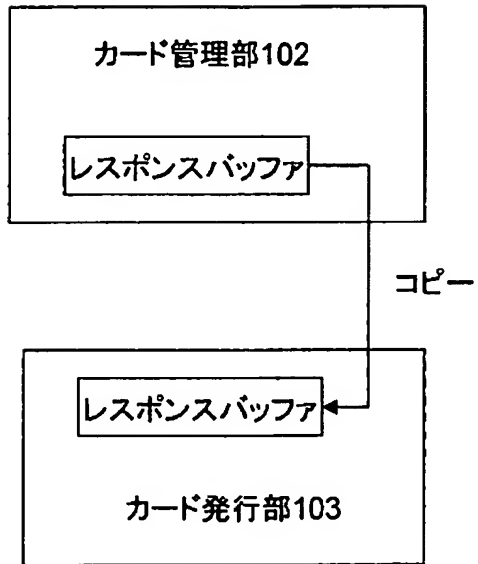




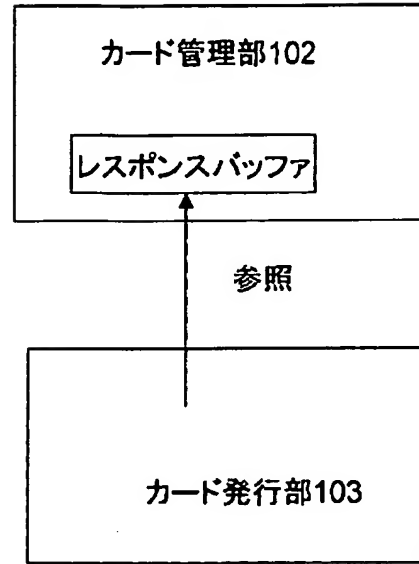
【図9】



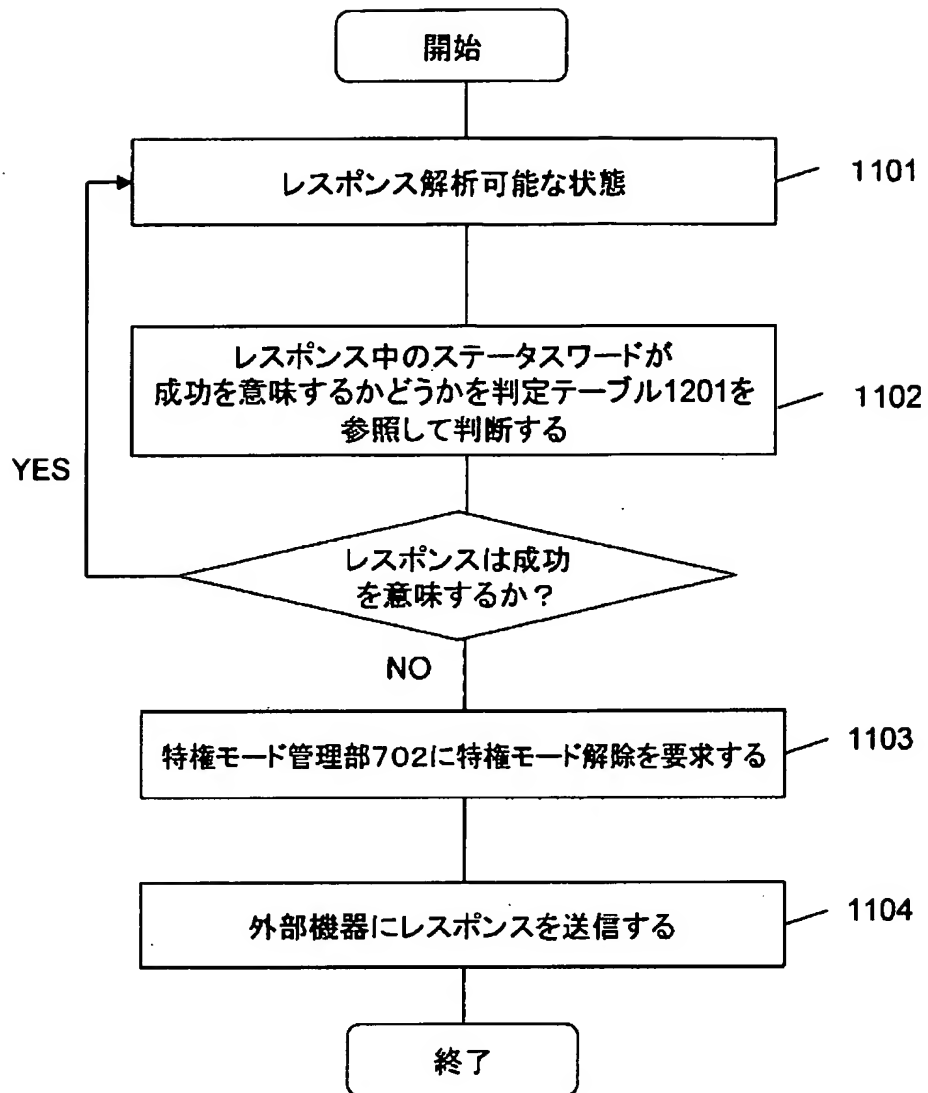
(a)



(b)



【図 11】

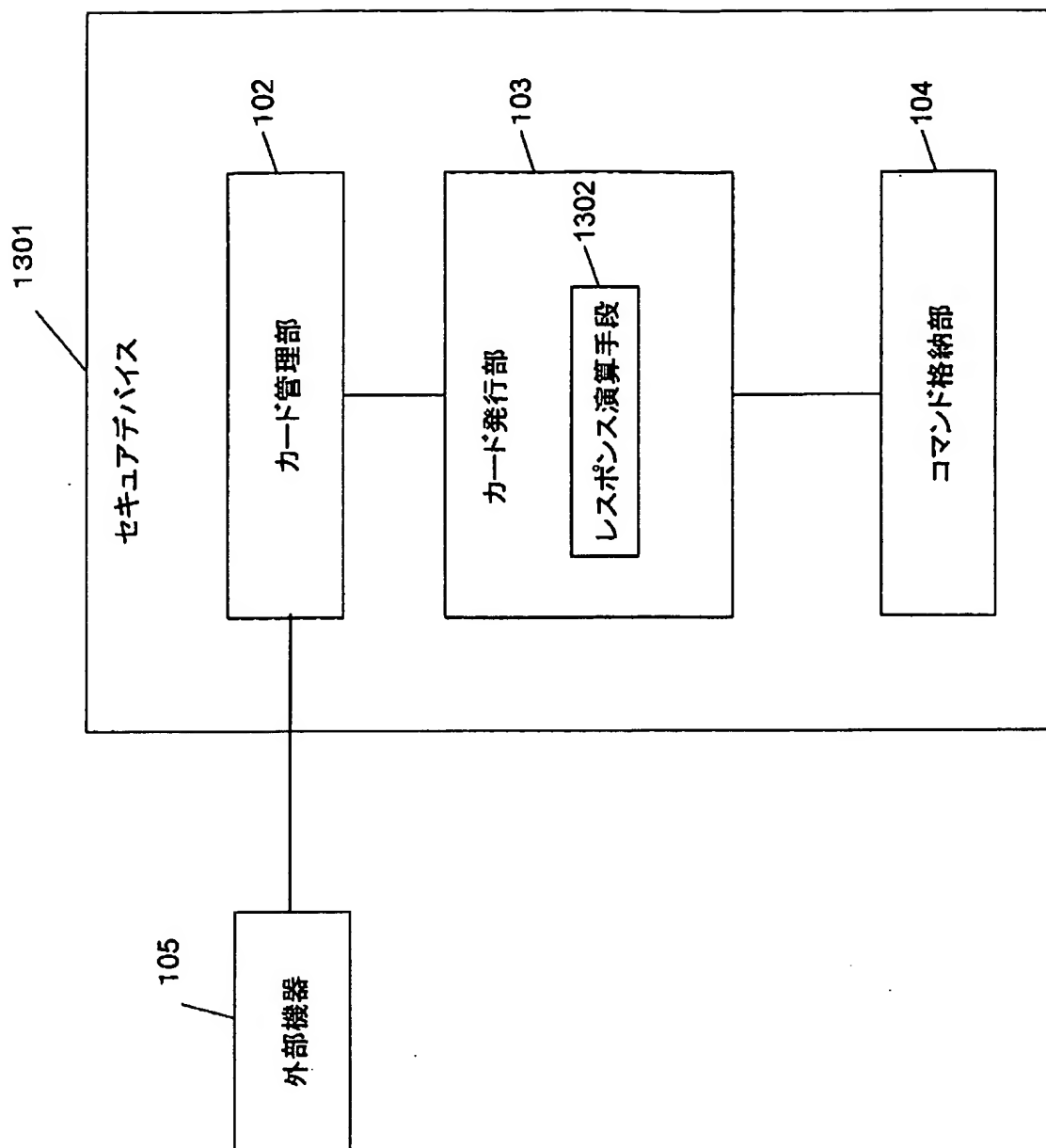


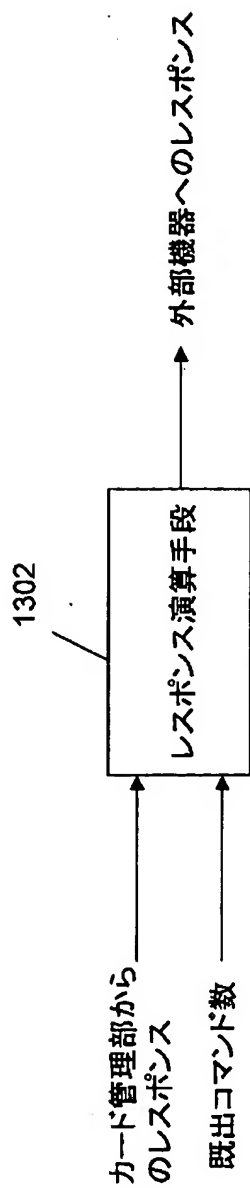
【図 1 2】

1201

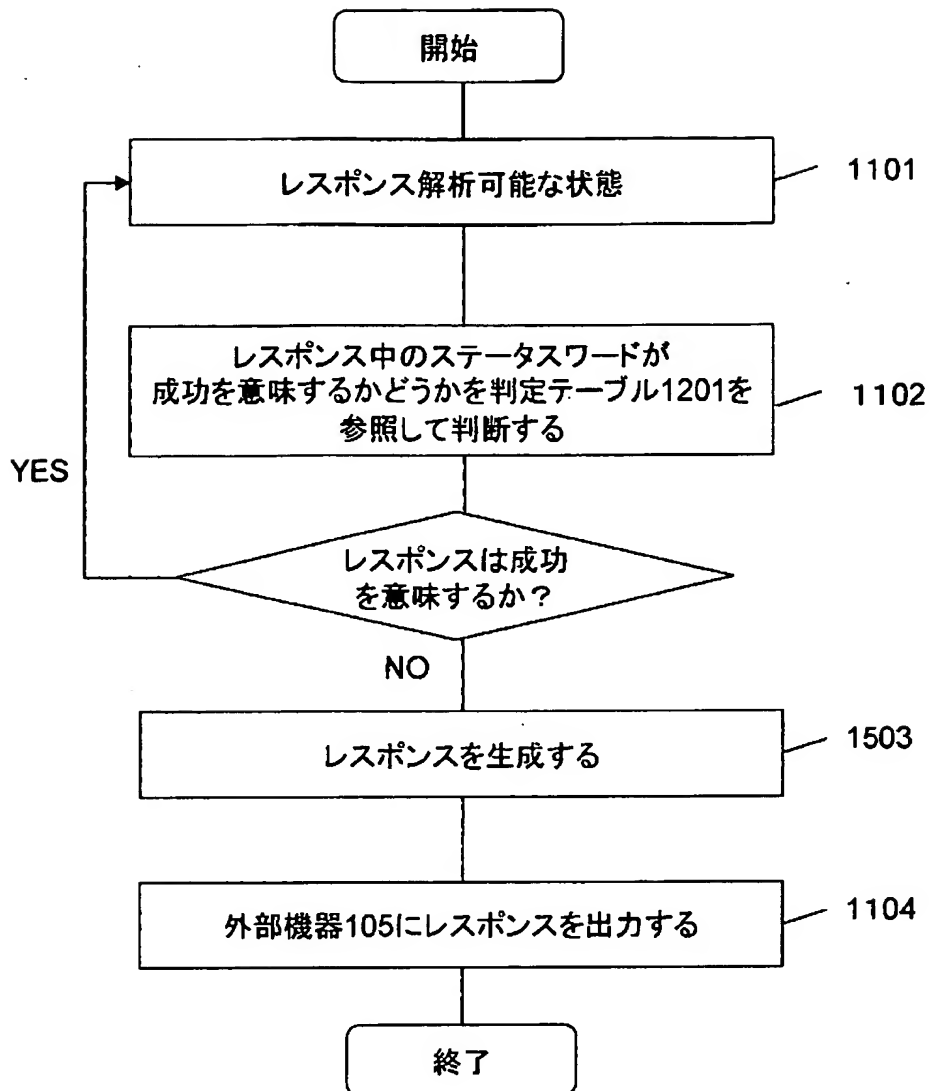
ステータスワード	結果
9000h	成功
9000h以外	失敗

【図 13】

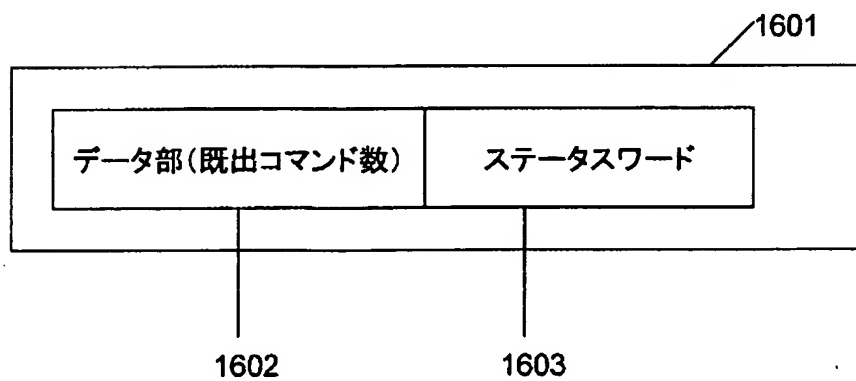


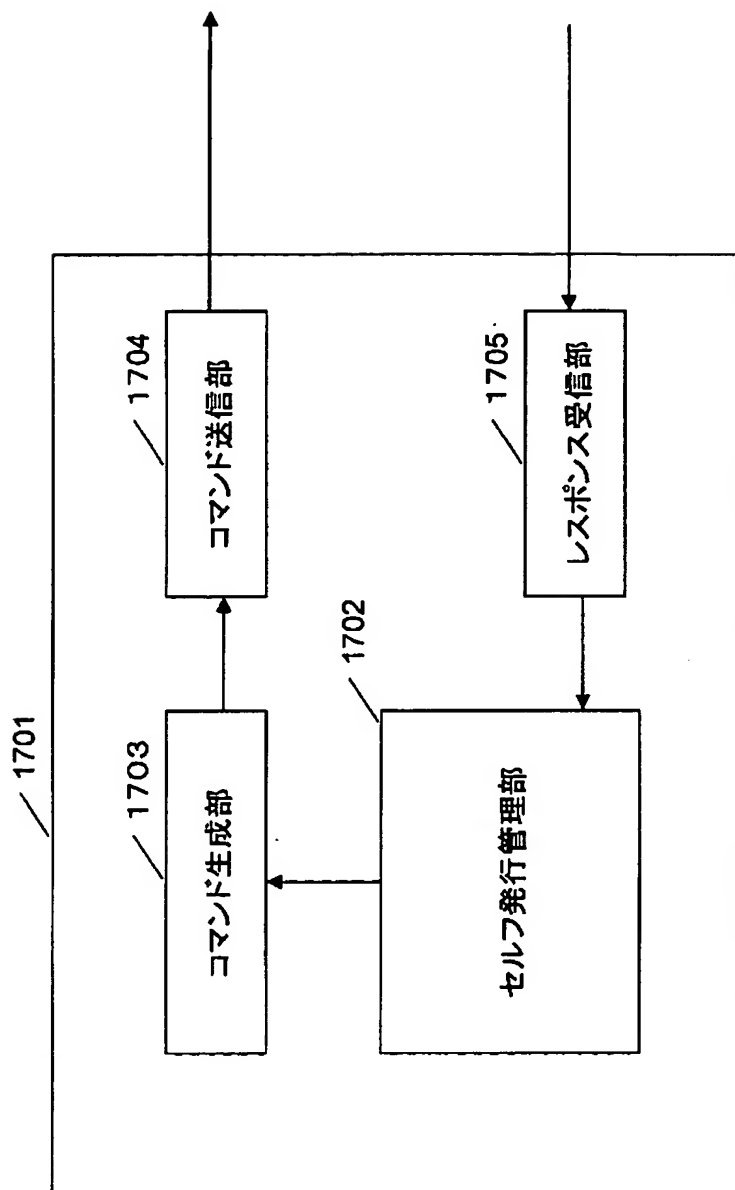


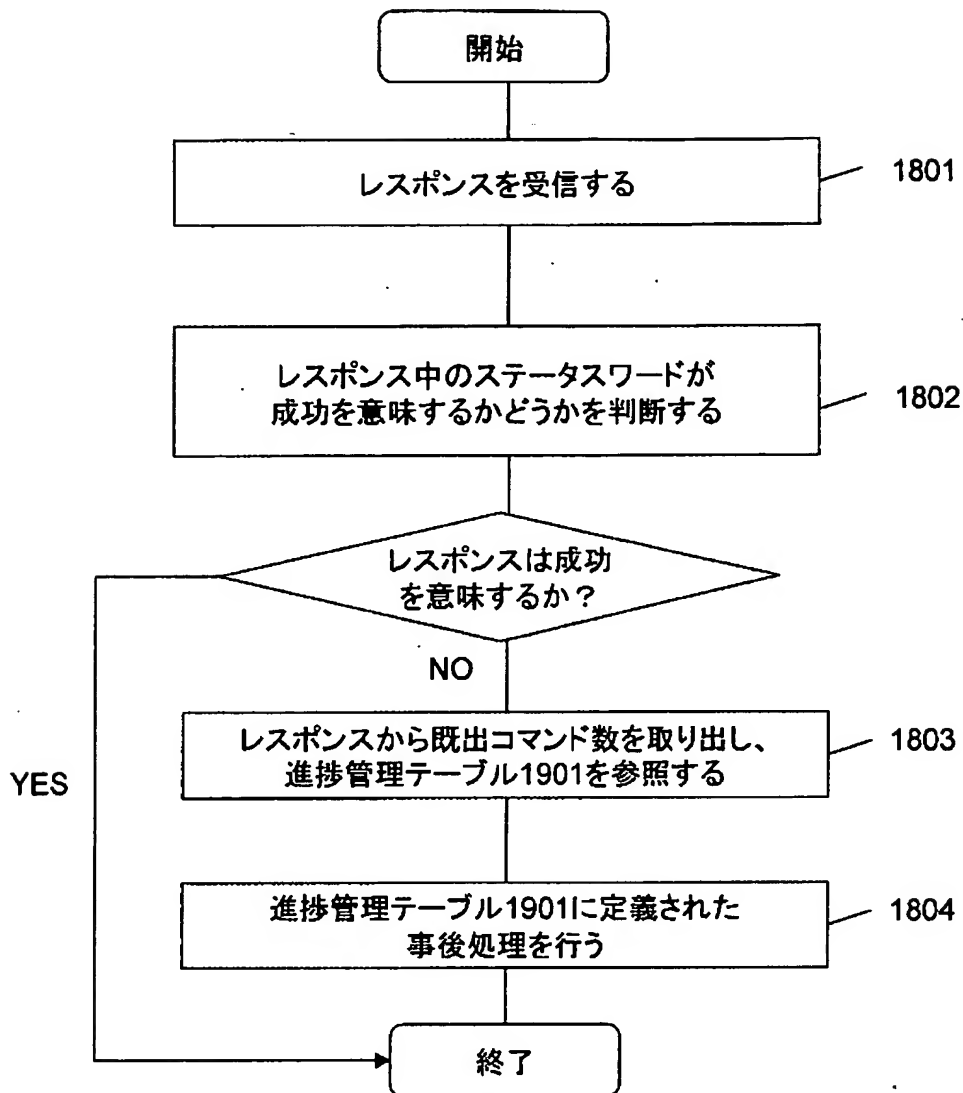
【図15】



【図16】





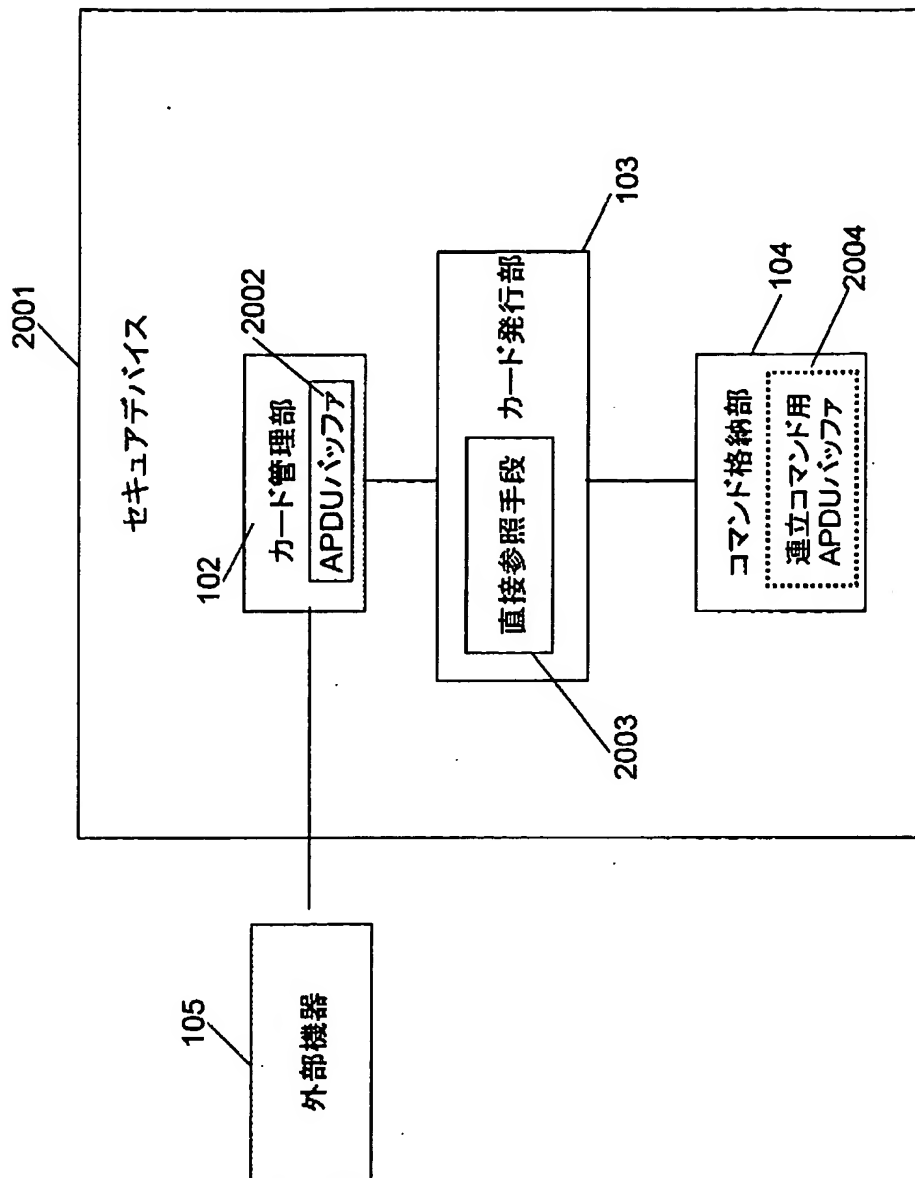


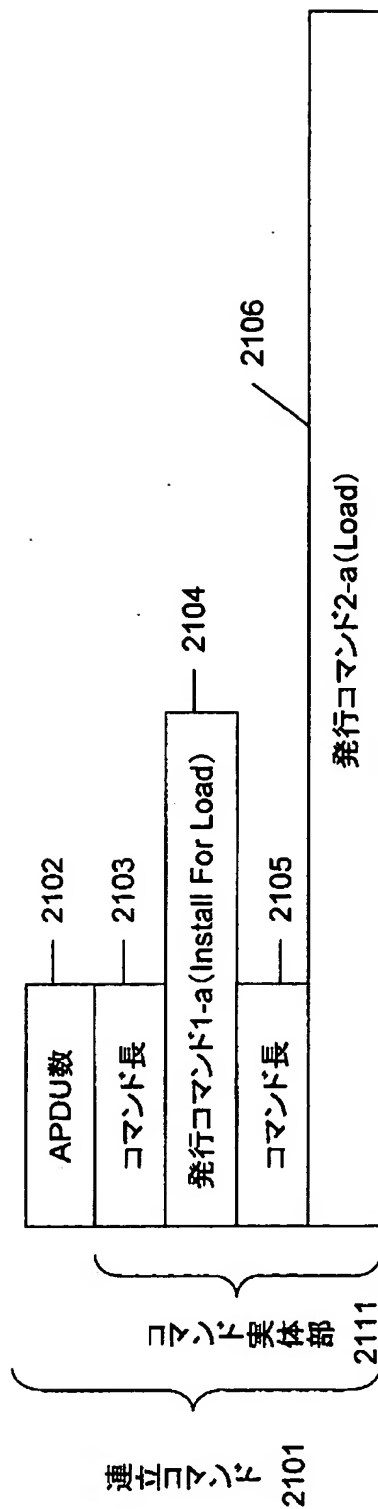
【図 19】

1901

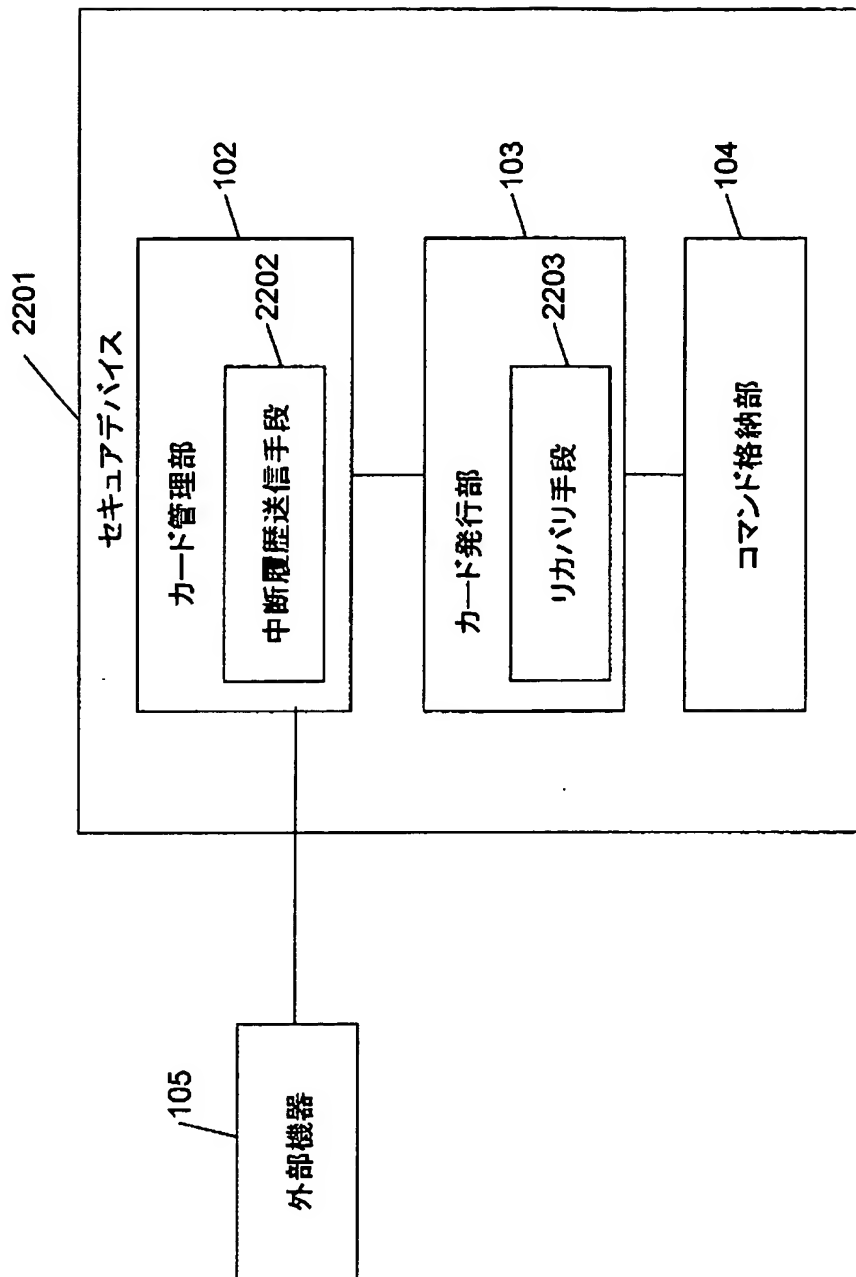
既出コマンド数	エラー処理
1	× × ×
2	△ △ △
.....
n	カードにクリアコマンド送信

【図20】

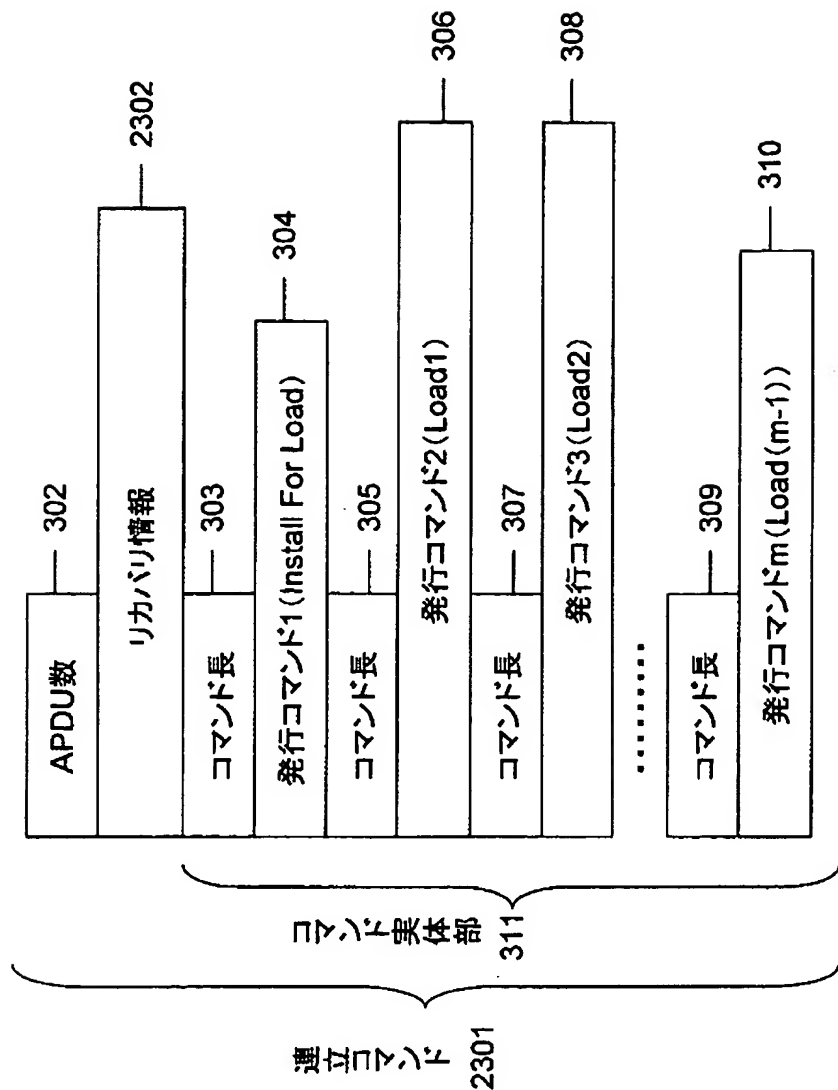


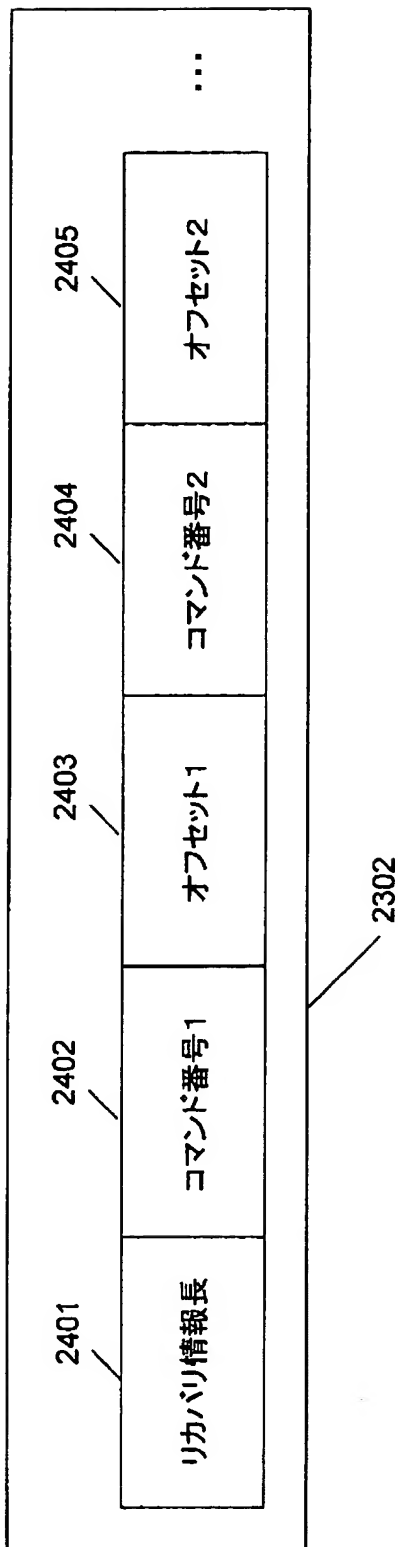


【図 2 2】

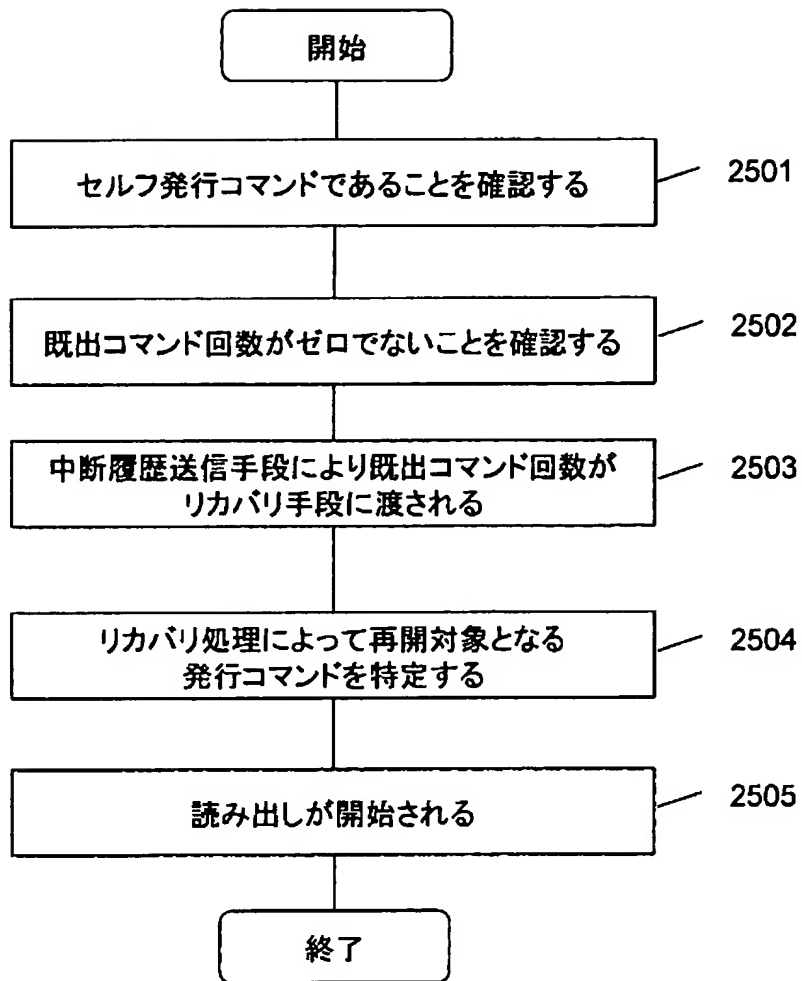


【図 2 3】

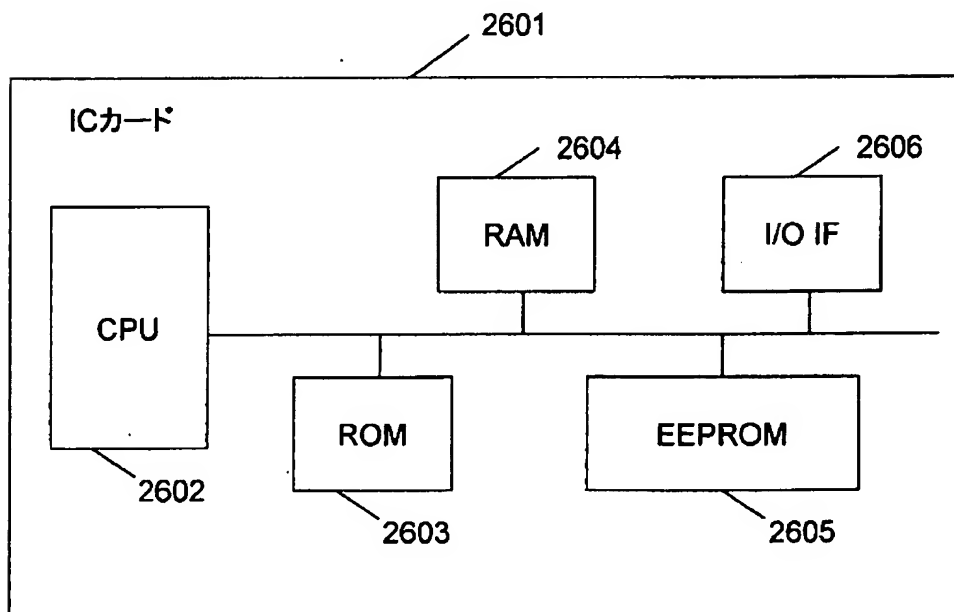




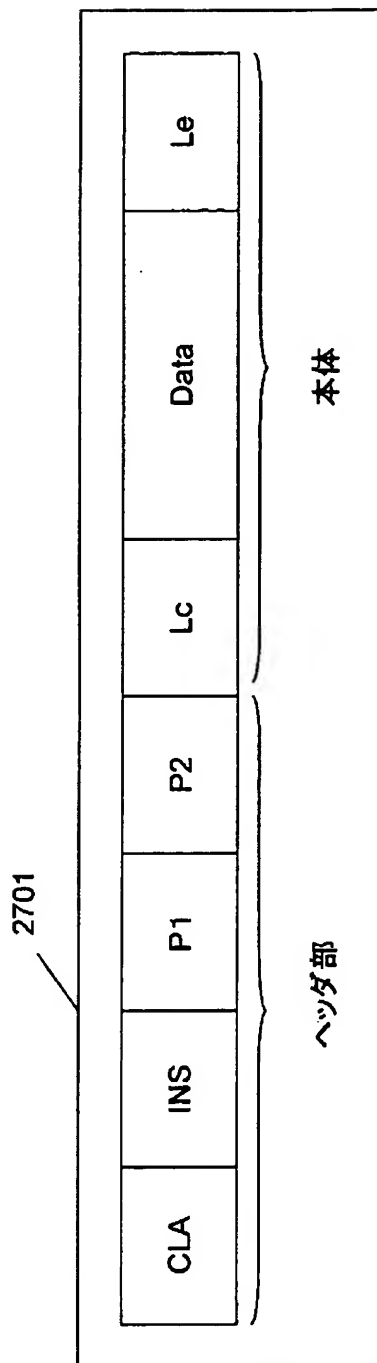
【図 2 5】



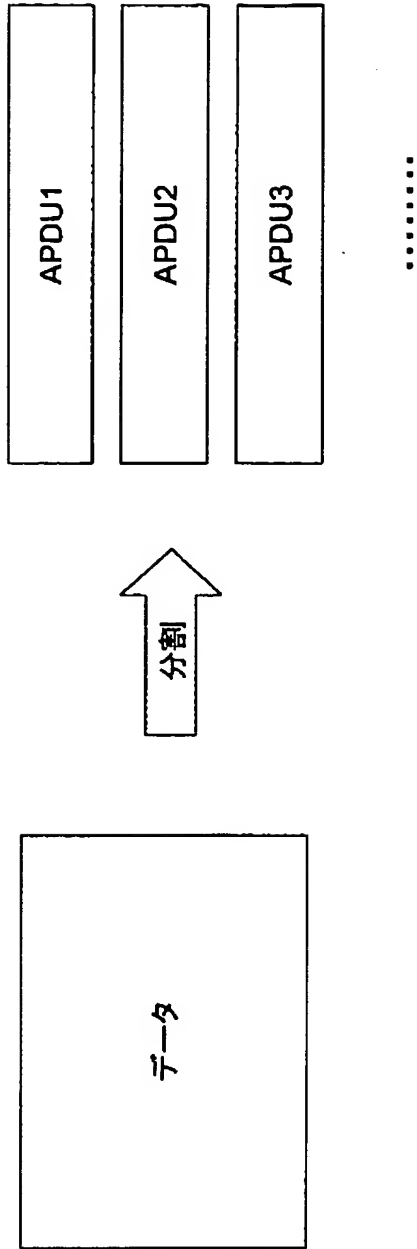
【図 2 6】



【図 2 7】



【図 2 8】



【書類名】要約書

【要約】

【課題】セキュアデバイスへのアプリケーションダウンロードを実行する場合に通信中断による発行処理の中断を防ぐとともに、外部機器から受信したセキュリティ対策を施したデータの処理負荷を軽減させることにより、アプリケーションダウンロードの高速化を実現するための装置およびその処理方法を提供する。

【解決手段】セキュアデバイスの動作を管理するカード管理部１０２が外部機器１０５からの指示を受けた後、カード発行部１０３がコマンド格納部１０４に保持された発行用コマンド群の中から指示をみたす一連の発行コマンドを選択、構築し、カード発行部１０３とカード管理部１０２との間で通信を実行し、発行を完了する。カード管理部１０２は、発行処理結果を外部機器１０５に出力する。

【選択図】図１

出願人履歴

0 0 0 0 0 5 8 2 1

19900828

新規登録

大阪府門真市大字門真1006番地

松下電器産業株式会社